Fig.1 (PRIOR ART)

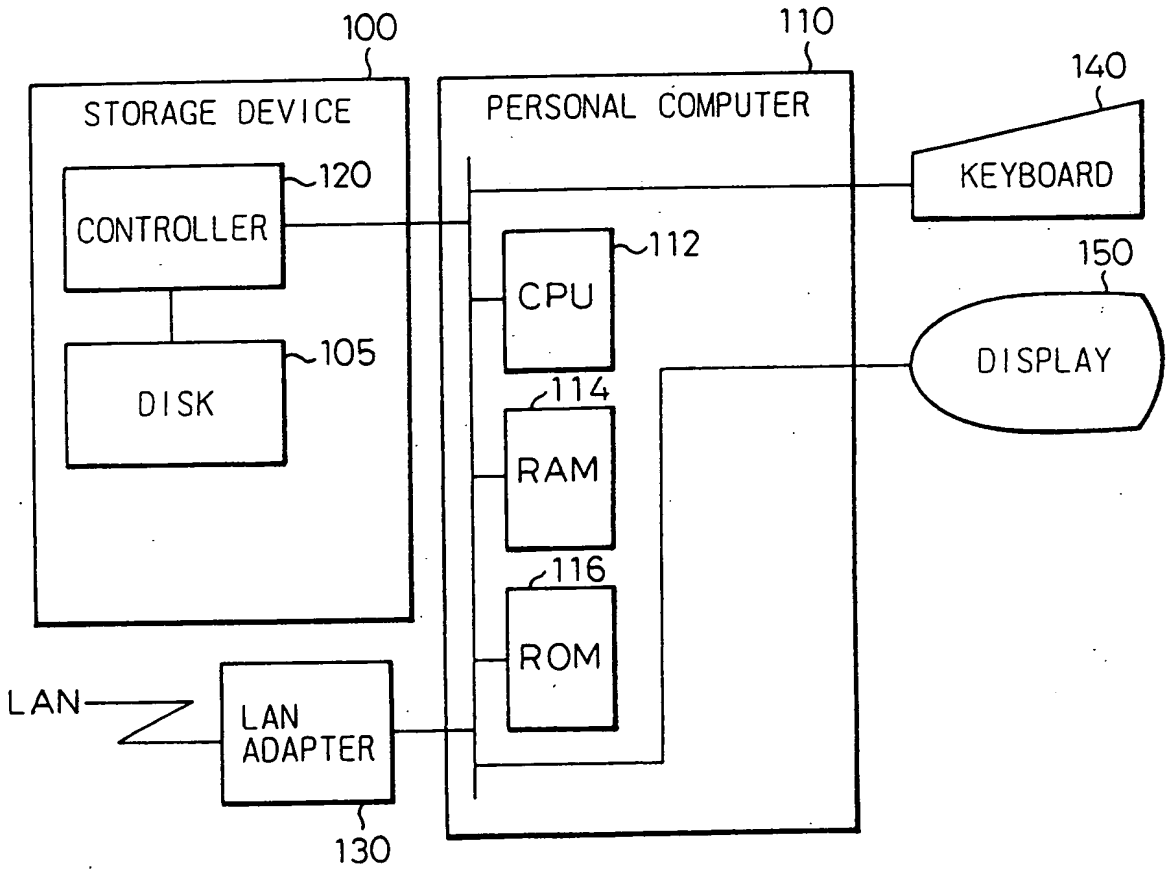


Fig.2

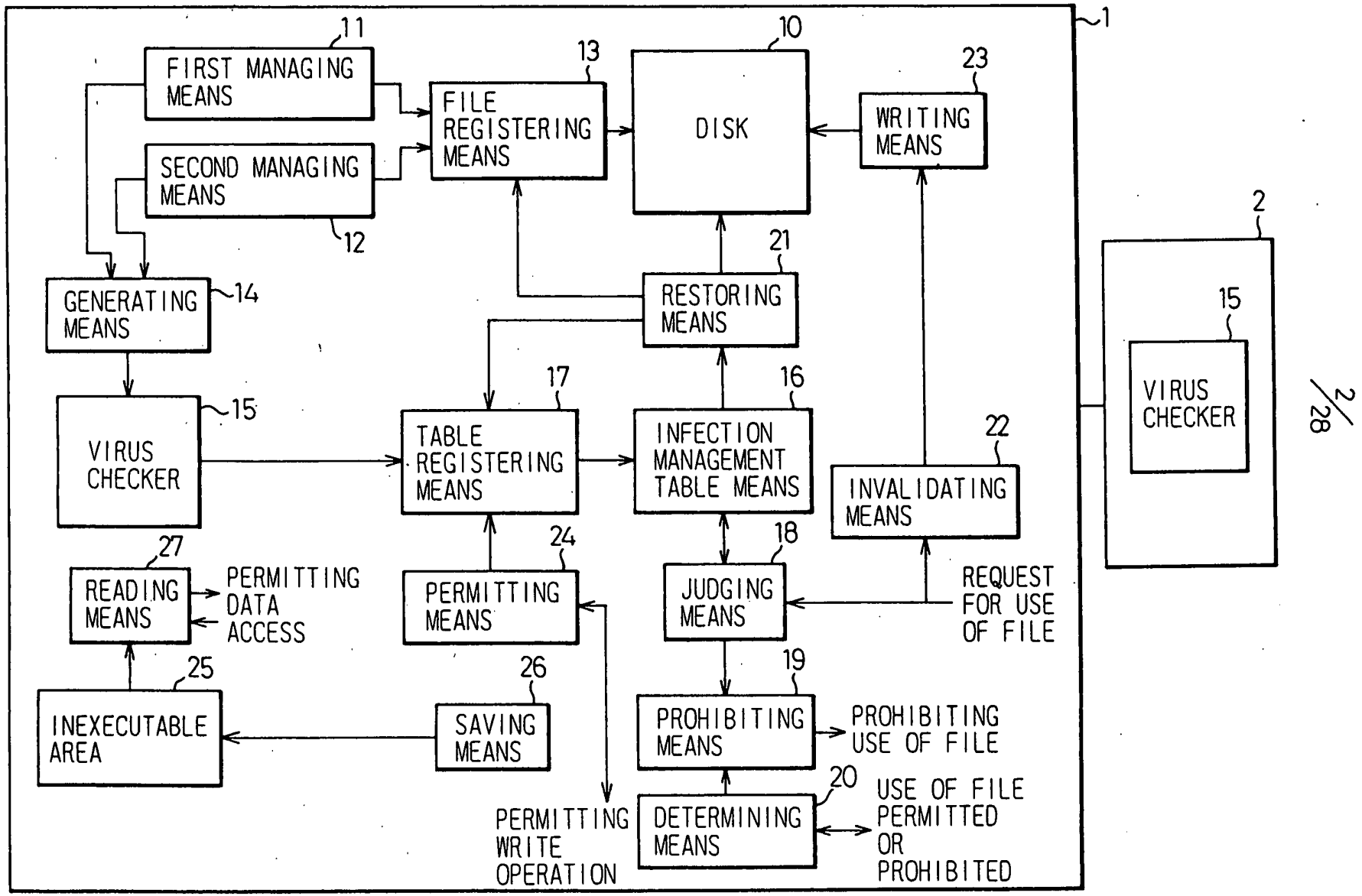

1
11
FIRST MANAGING MEANS
SECOND MANAGING MEANS
12
13
FILE REGISTERING MEANS
10
DISK
23
WRITING MEANS
2
15
VIRUS CHECKER
21
RESTORING MEANS
14
GENERATING MEANS
15
VIRUS CHECKER
17
TABLE REGISTERING MEANS
16
INFECTION MANAGEMENT TABLE MEANS
22
INVALIDATING MEANS
27
READING MEANS
PERMITTING DATA ACCESS
24
PERMITTING MEANS
18
JUDGING MEANS
REQUEST FOR USE OF FILE
25
INEXECUTABLE AREA
26
SAVING MEANS
19
PROHIBITING MEANS
PROHIBITING USE OF FILE
20
DETERMINING MEANS
USE OF FILE PERMITTED OR PROHIBITED
PERMITTING WRITE OPERATION

Fig.3

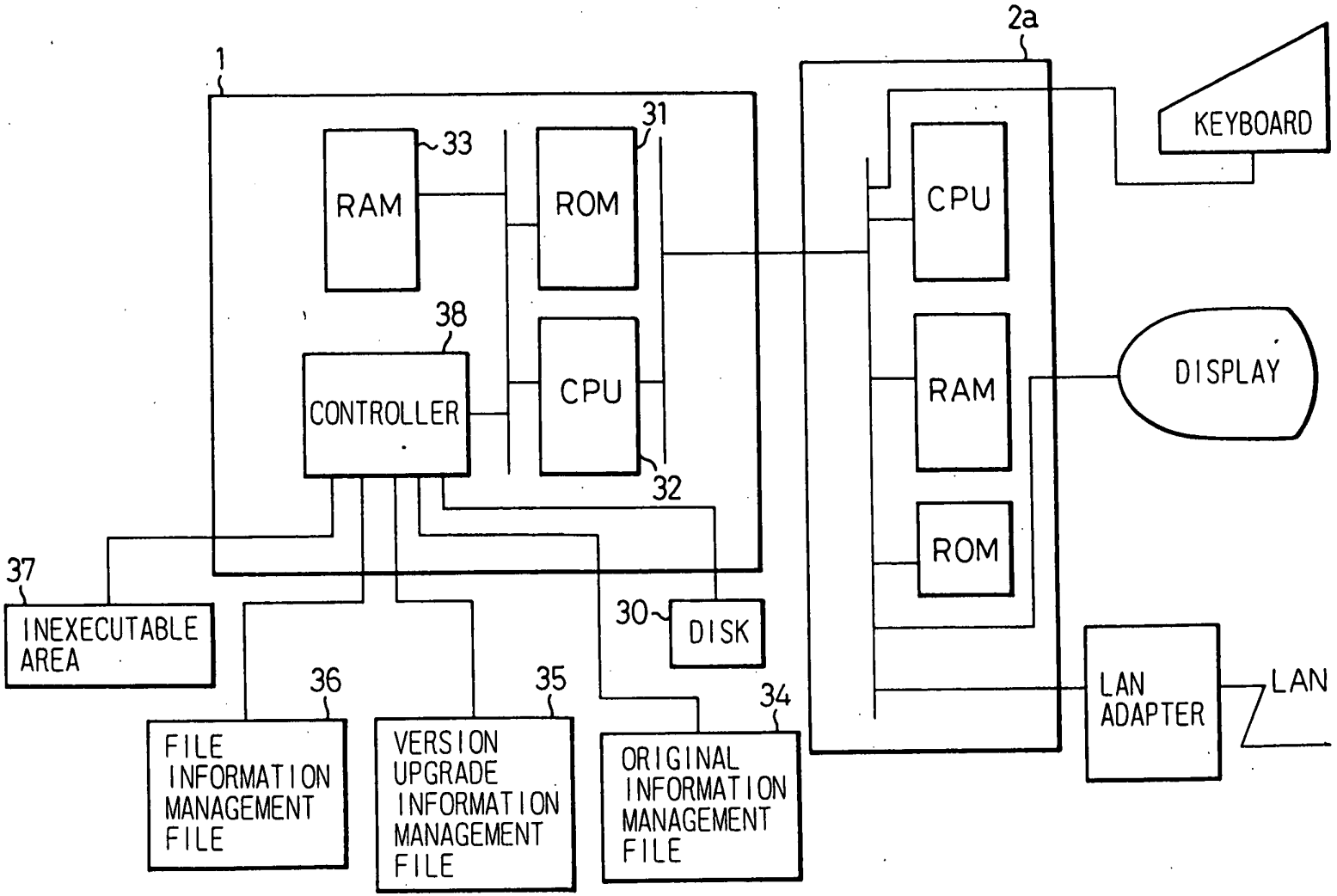

1
2a
RAM
33
ROM
31
CPU
KEYBOARD
38
CONTROLLER
CPU
32
RAM
DISPLAY
ROM
37
INEXECUTABLE AREA
30
DISK
LAN ADAPTER
LAN
36
35
34
FILE INFORMATION MANAGEMENT FILE
VERSION UPGRADE INFORMATION MANAGEMENT FILE
ORIGINAL INFORMATION MANAGEMENT FILE

Fig.4

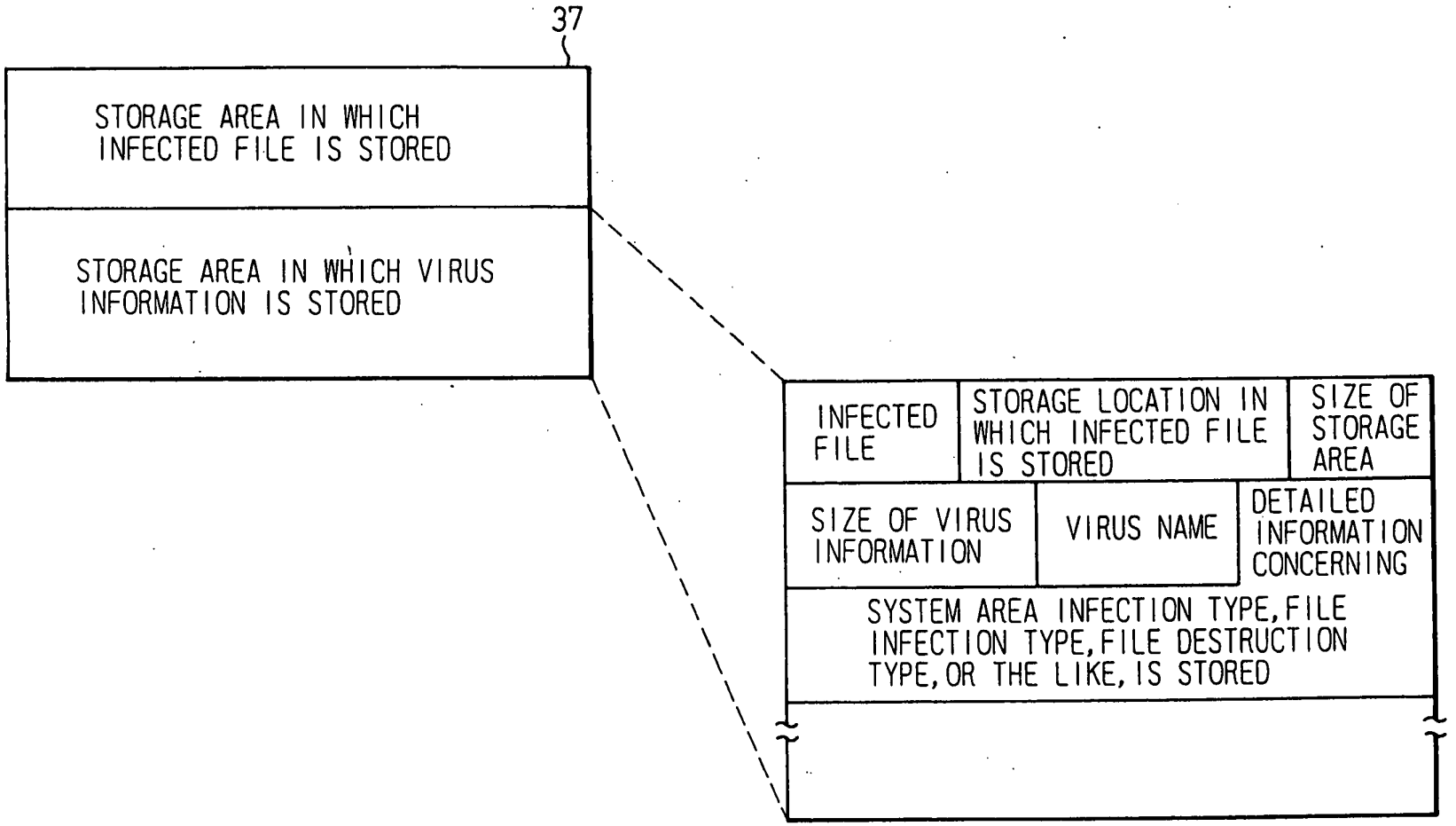

37
STORAGE AREA IN WHICH INFECTED FILE IS STORED
STORAGE AREA IN WHICH VIRUS INFORMATION IS STORED
INFECTED FILE
STORAGE LOCATION IN WHICH INFECTED FILE IS STORED
SIZE OF STORAGE AREA
SIZE OF VIRUS INFORMATION
VIRUS NAME
DETAILED INFORMATION CONCERNING
SYSTEM AREA INFECTION TYPE, FILE INFECTION TYPE, FILE DESTRUCTION TYPE, OR THE LIKE, IS STORED

Fig.5

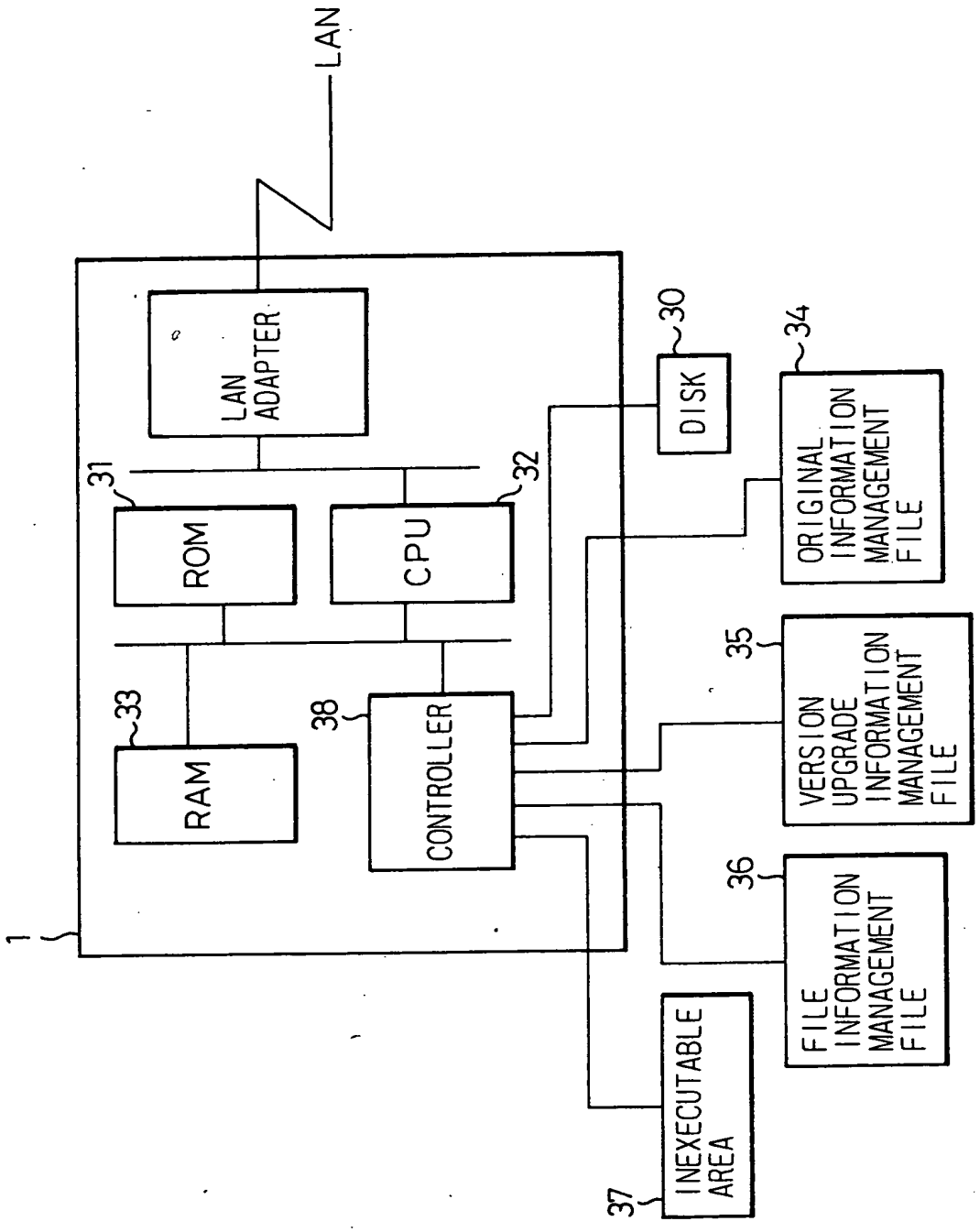

LAN
LAN ADAPTER
ROM
CPU
RAM
CONTROLLER
DISK
ORIGINAL INFORMATION MANAGEMENT FILE
VERSION UPGRADE INFORMATION MANAGEMENT FILE
FILE INFORMATION MANAGEMENT FILE
INEXECUTABLE AREA
1
30
31
32
33
34
35
36
37
38

Fig.6

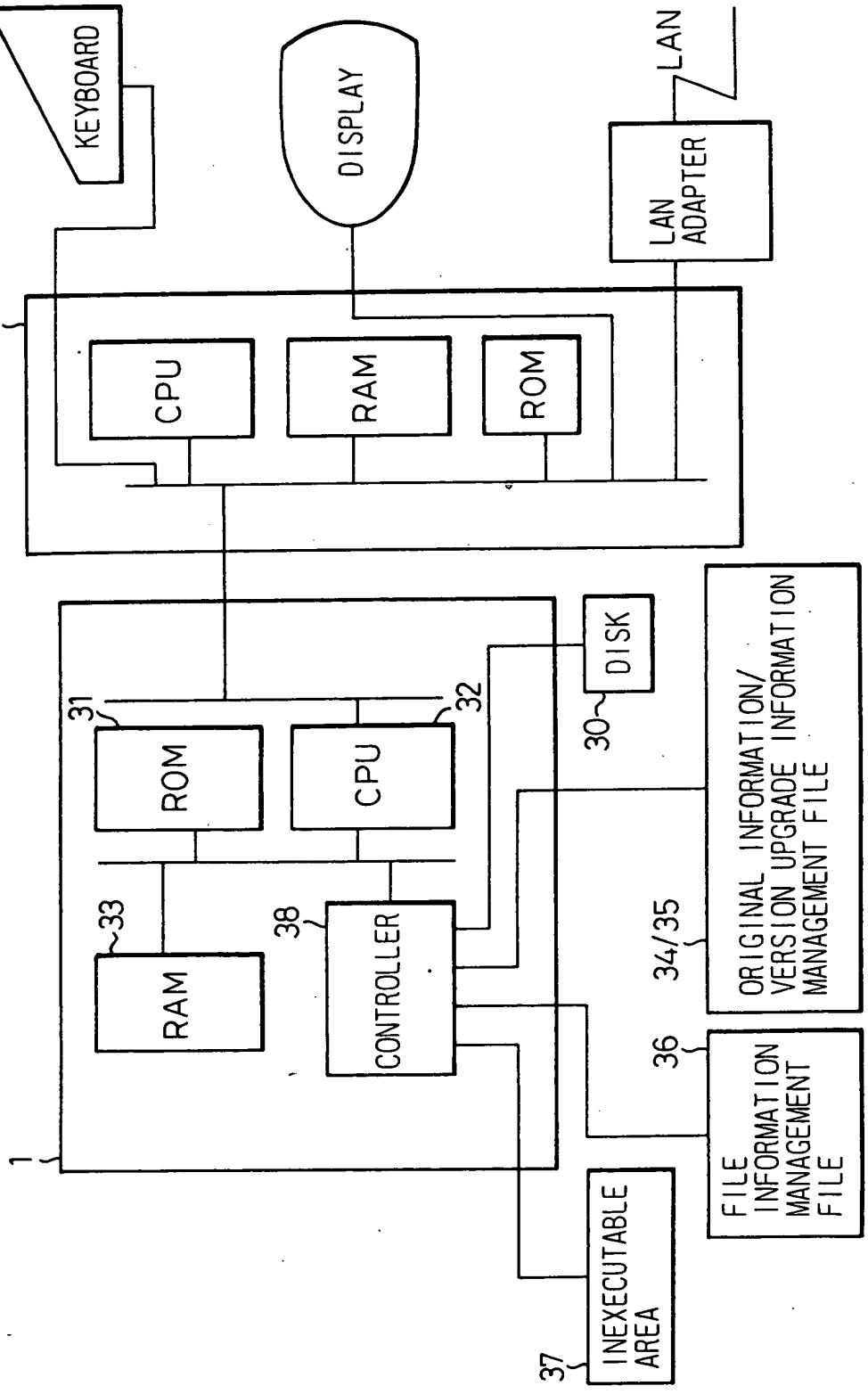

KEYBOARD
DISPLAY
LAN
LAN ADAPTER
2a
CPU
RAM
ROM
1
31
ROM
32
CPU
DISK
30
33
RAM
38
CONTROLLER
34/35
ORIGINAL INFORMATION/ VERSION UPGRADE INFORMATION MANAGEMENT FILE
36
FILE INFORMATION MANAGEMENT FILE
37
INEXECUTABLE AREA

Fig.7

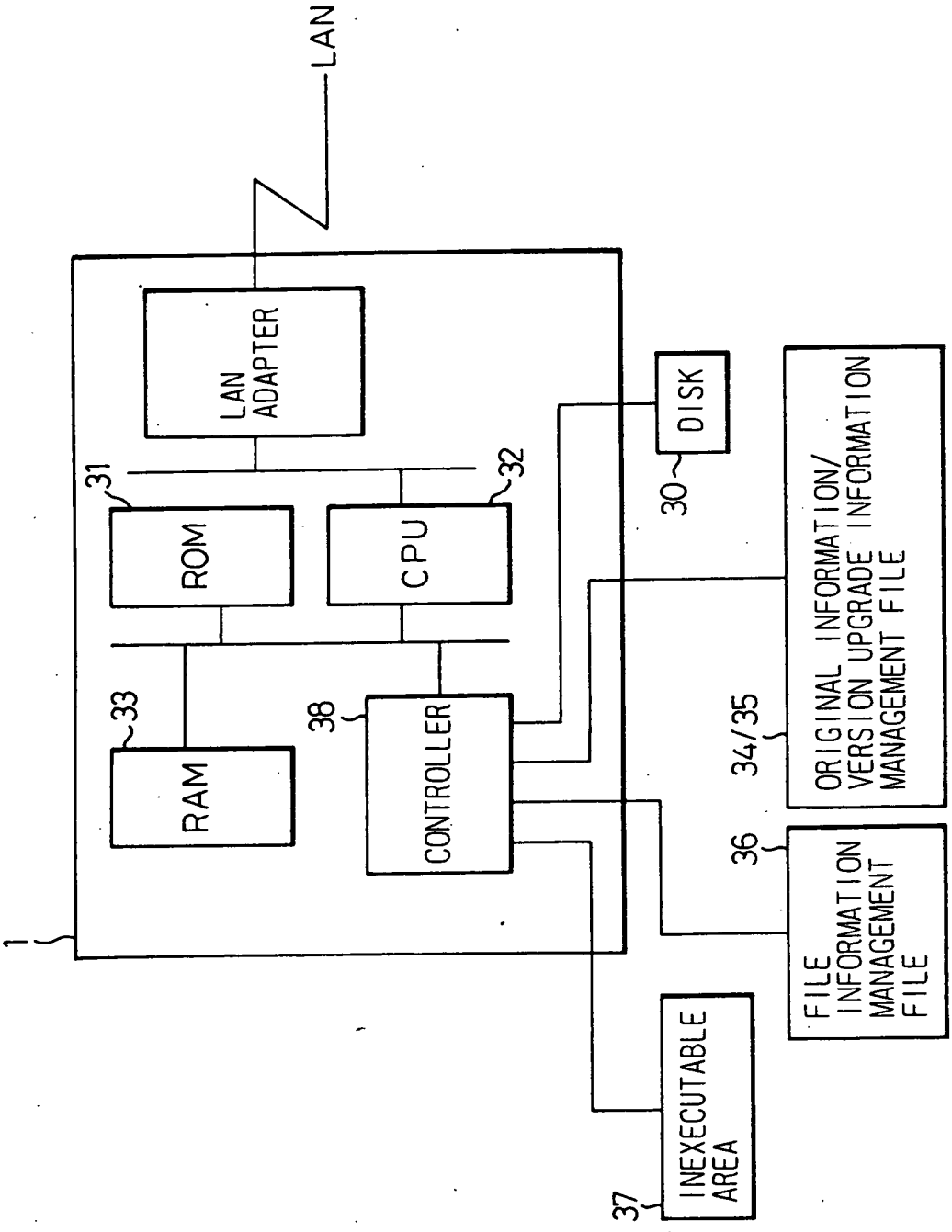

LAN
LAN ADAPTER
ROM
CPU
RAM
CONTROLLER
DISK
ORIGINAL INFORMATION/ VERSION UPGRADE INFORMATION MANAGEMENT FILE
FILE INFORMATION MANAGEMENT FILE
INEXECUTABLE AREA
1
30
31
32
33
34/35
36
37
38

Fig.8

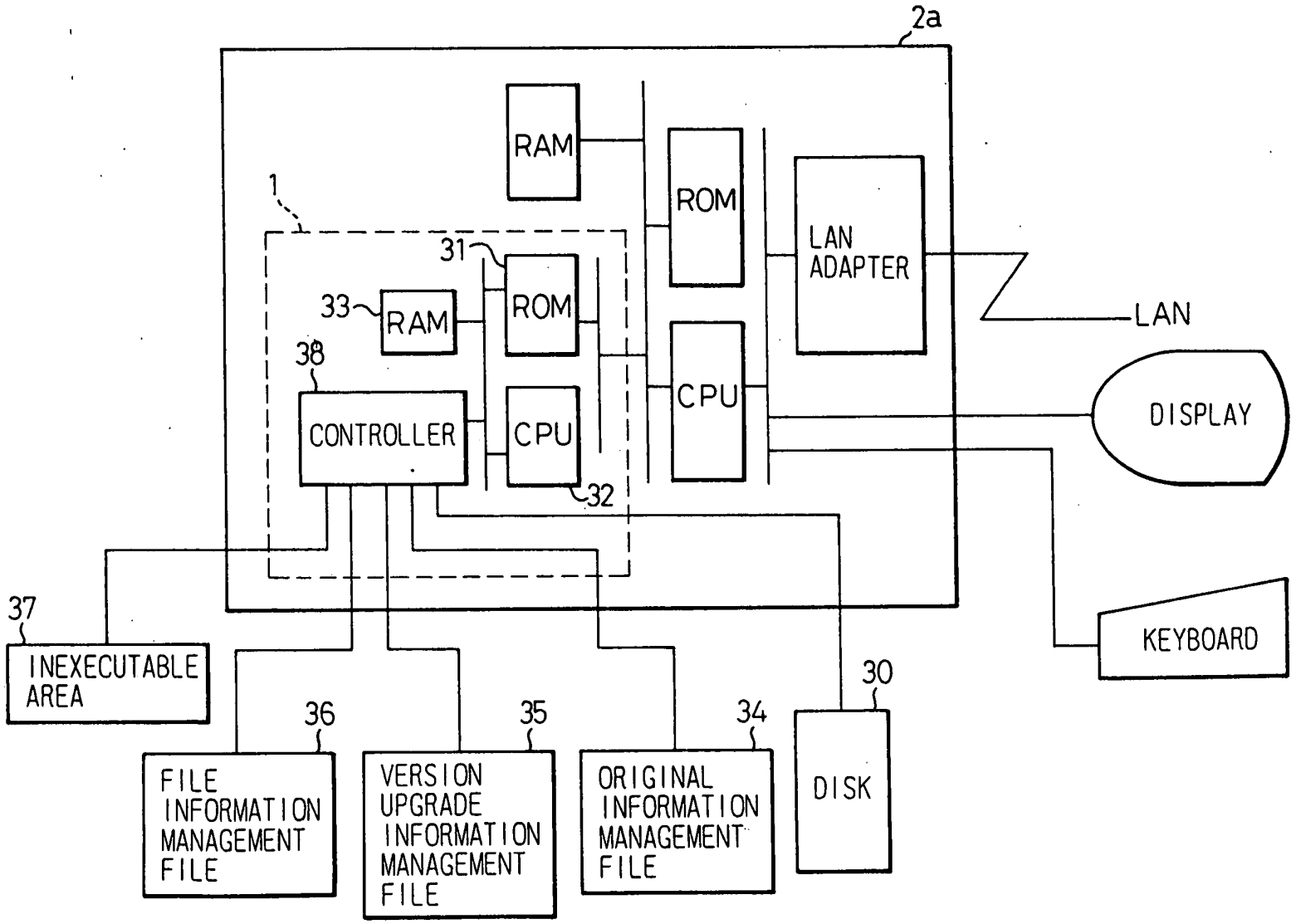

2a
RAM
ROM
LAN ADAPTER
LAN
1
31
ROM
33
RAM
38
CONTROLLER
CPU
32
CPU
DISPLAY
KEYBOARD
37
INEXECUTABLE AREA
36
FILE INFORMATION MANAGEMENT FILE
35
VERSION UPGRADE INFORMATION MANAGEMENT FILE
34
ORIGINAL INFORMATION MANAGEMENT FILE
30
DISK

Fig.9

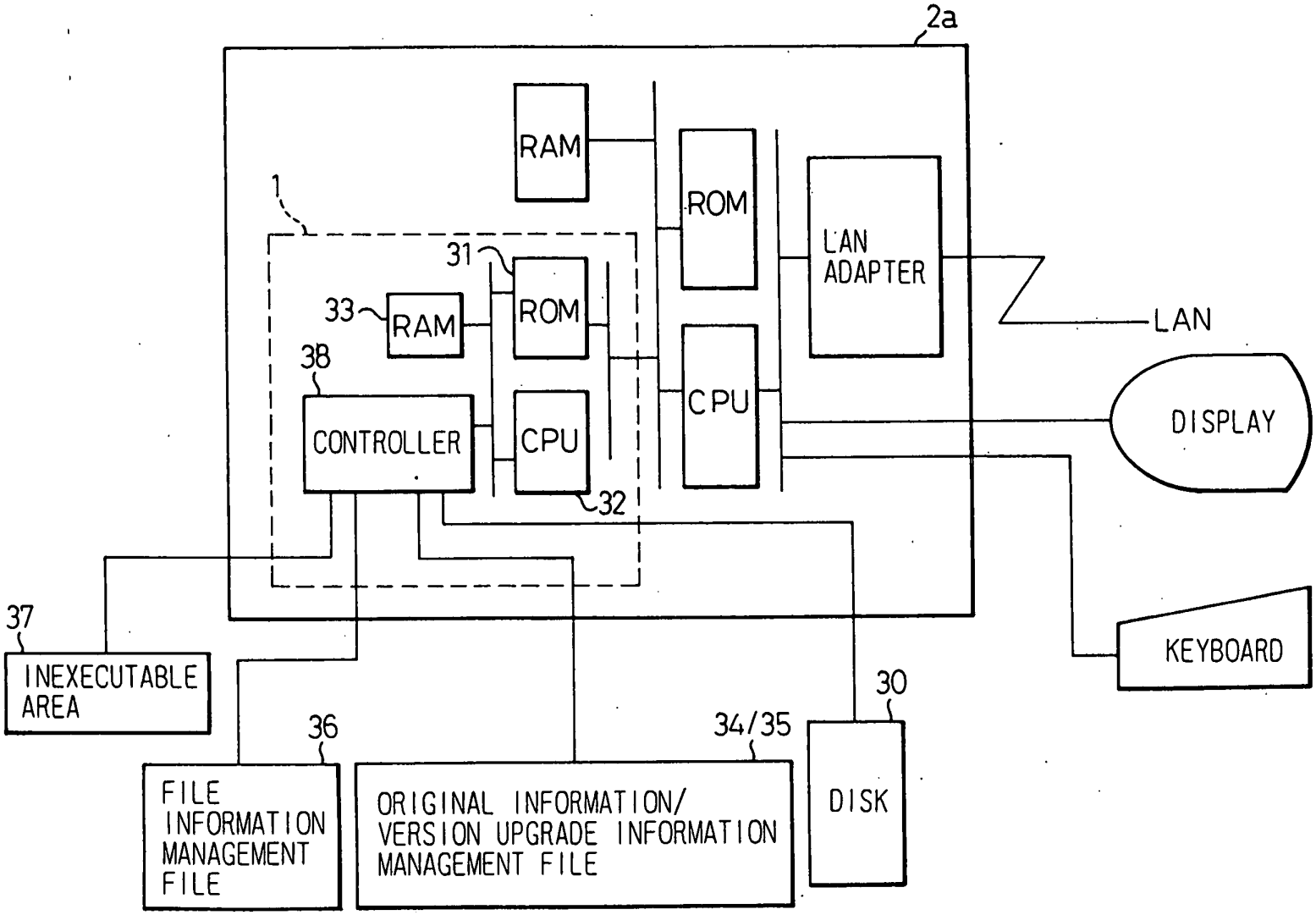

2a
RAM
ROM
LAN ADAPTER
LAN
1
31
33
RAM
ROM
38
CONTROLLER
CPU
CPU
32
DISPLAY
KEYBOARD
37
INEXECUTABLE AREA
30
36
34/35
FILE INFORMATION MANAGEMENT FILE
ORIGINAL INFORMATION/ VERSION UPGRADE INFORMATION MANAGEMENT FILE
DISK

Fig.10

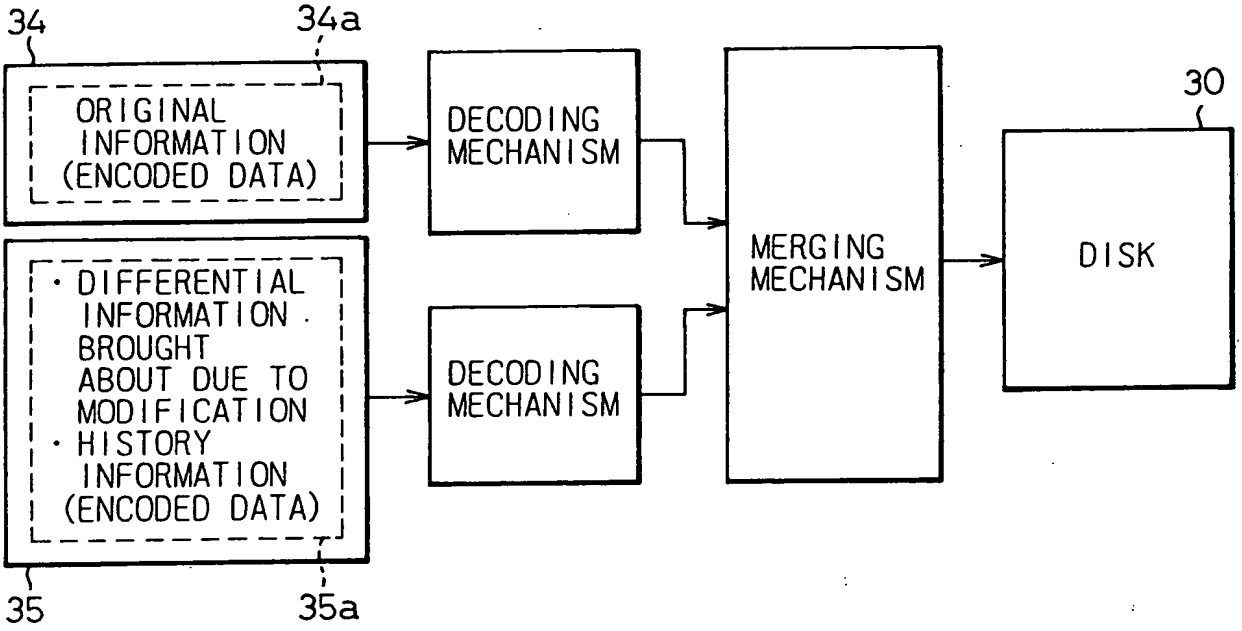

34
34a
ORIGINAL INFORMATION (ENCODED DATA)
DECODING MECHANISM
MERGING MECHANISM
30
DISK
· DIFFERENTIAL INFORMATION BROUGHT ABOUT DUE TO MODIFICATION
· HISTORY INFORMATION (ENCODED DATA)
DECODING MECHANISM
35
35a

Fig.11

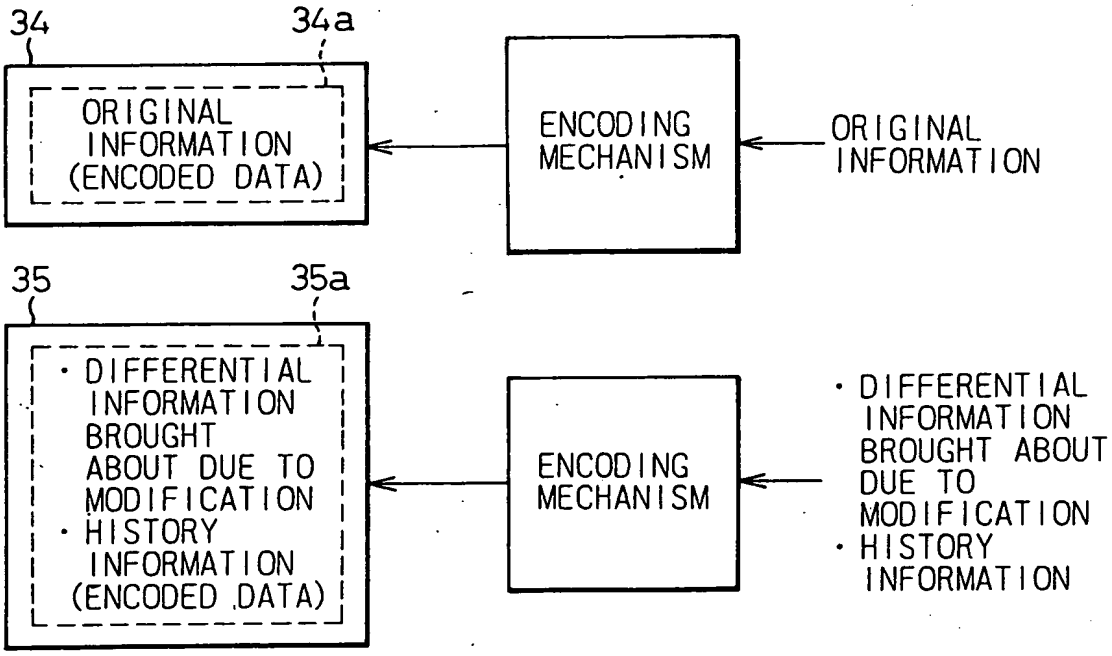

34
34a
ORIGINAL INFORMATION (ENCODED DATA)
ENCODING MECHANISM
ORIGINAL INFORMATION
35
35a
· DIFFERENTIAL INFORMATION BROUGHT ABOUT DUE TO MODIFICATION
· HISTORY INFORMATION (ENCODED DATA)
ENCODING MECHANISM
· DIFFERENTIAL INFORMATION BROUGHT ABOUT DUE TO MODIFICATION
· HISTORY INFORMATION

Fig.12

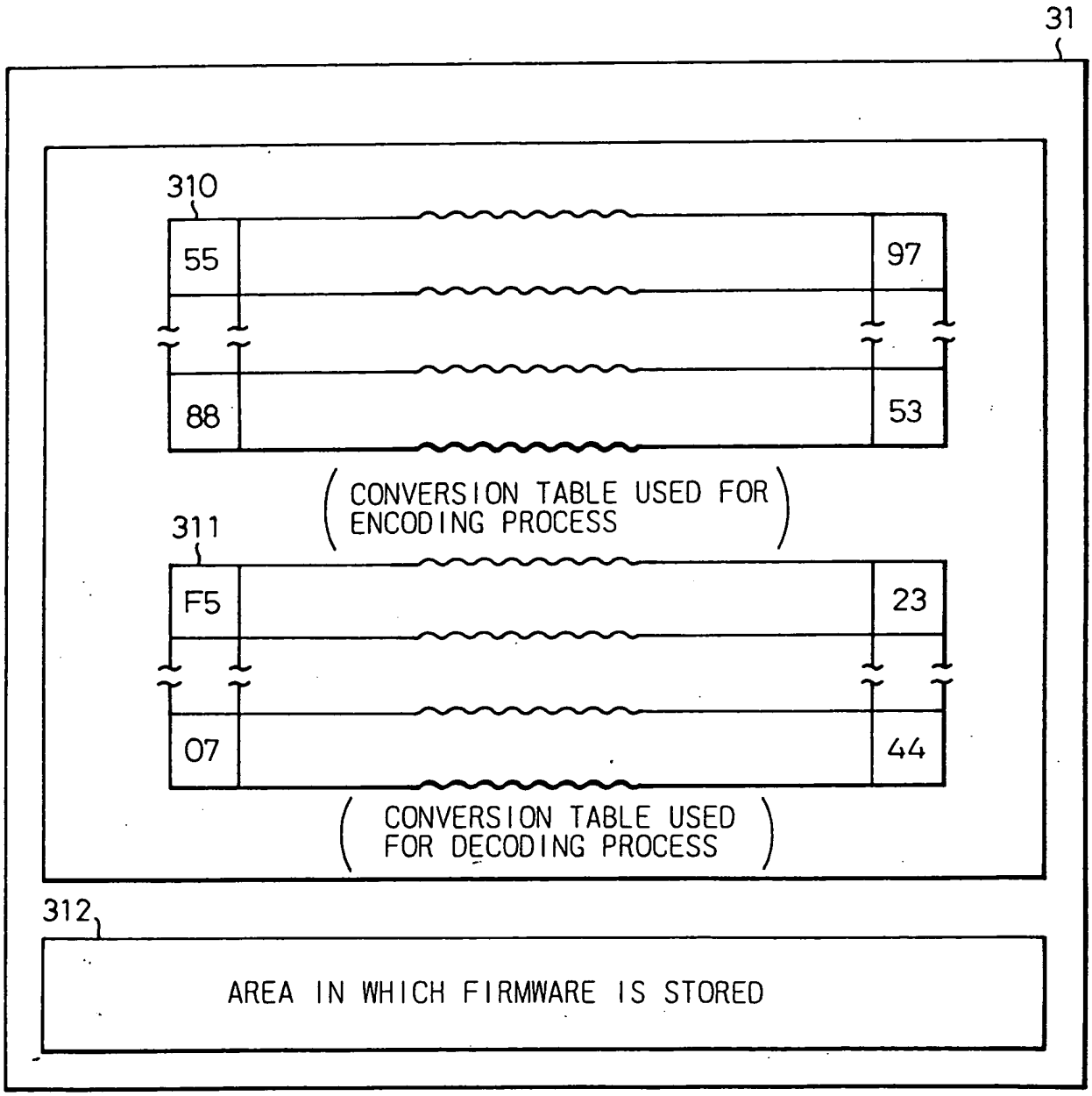

31
310
55
97
88
53
CONVERSION TABLE USED FOR ENCODING PROCESS
311
F5
23
07
44
CONVERSION TABLE USED FOR DECODING PROCESS
312
AREA IN WHICH FIRMWARE IS STORED

Fig.13

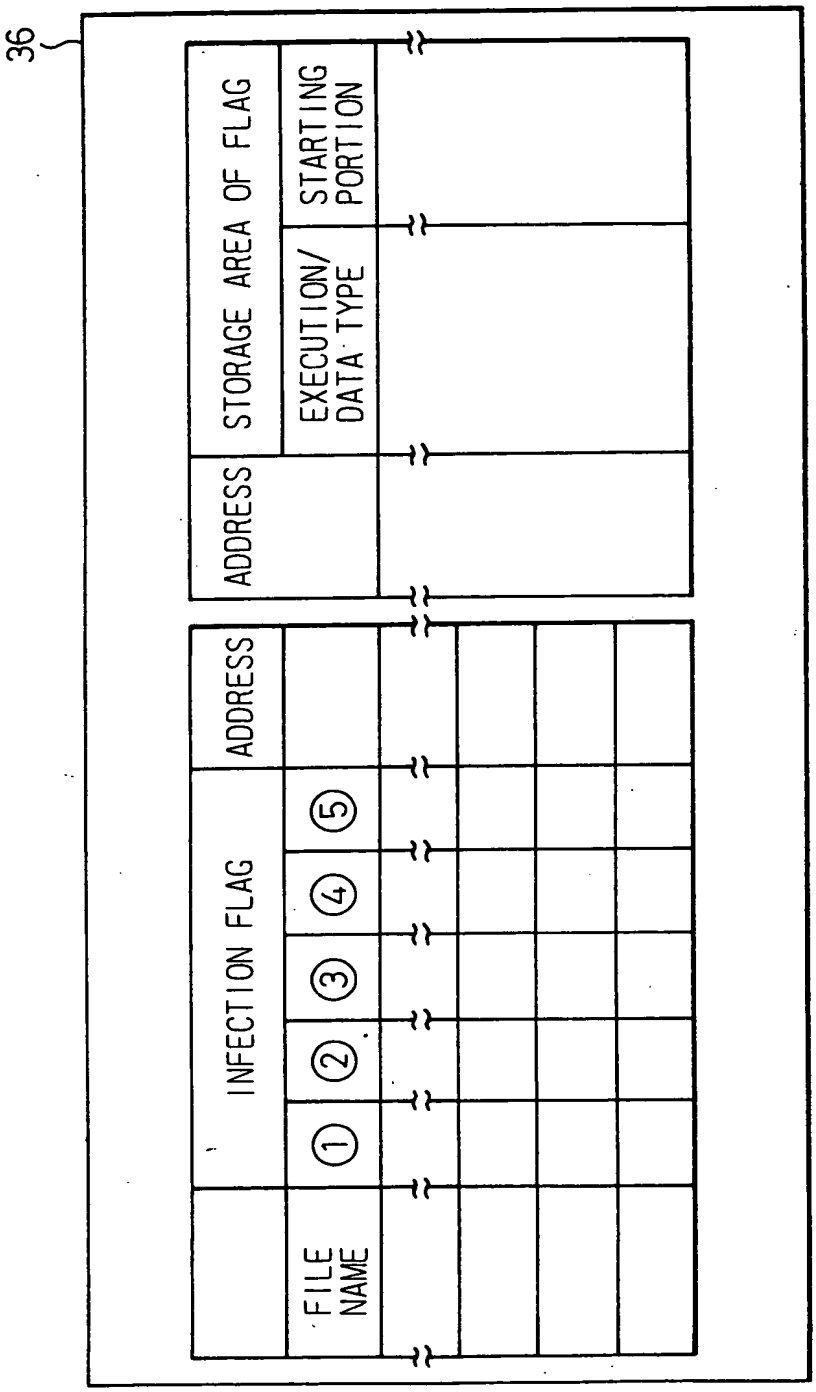

36
FILE NAME
INFECTION FLAG
①
②
③
④
⑤
ADDRESS
ADDRESS
STORAGE AREA OF FLAG
EXECUTION/ DATA TYPE
STARTING PORTION

Fig.14

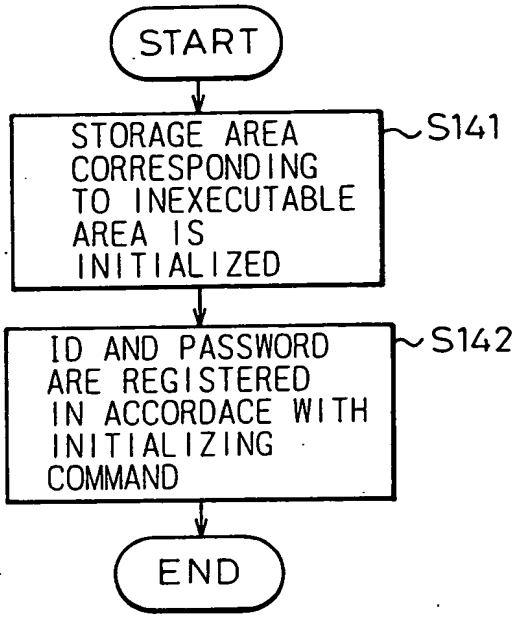

START
STORAGE AREA CORRESPONDING TO INEXECUTABLE AREA IS INITIALIZED
S141
ID AND PASSWORD ARE REGISTERED IN ACCORDACE WITH INITIALIZING COMMAND
S142
END

Fig.15

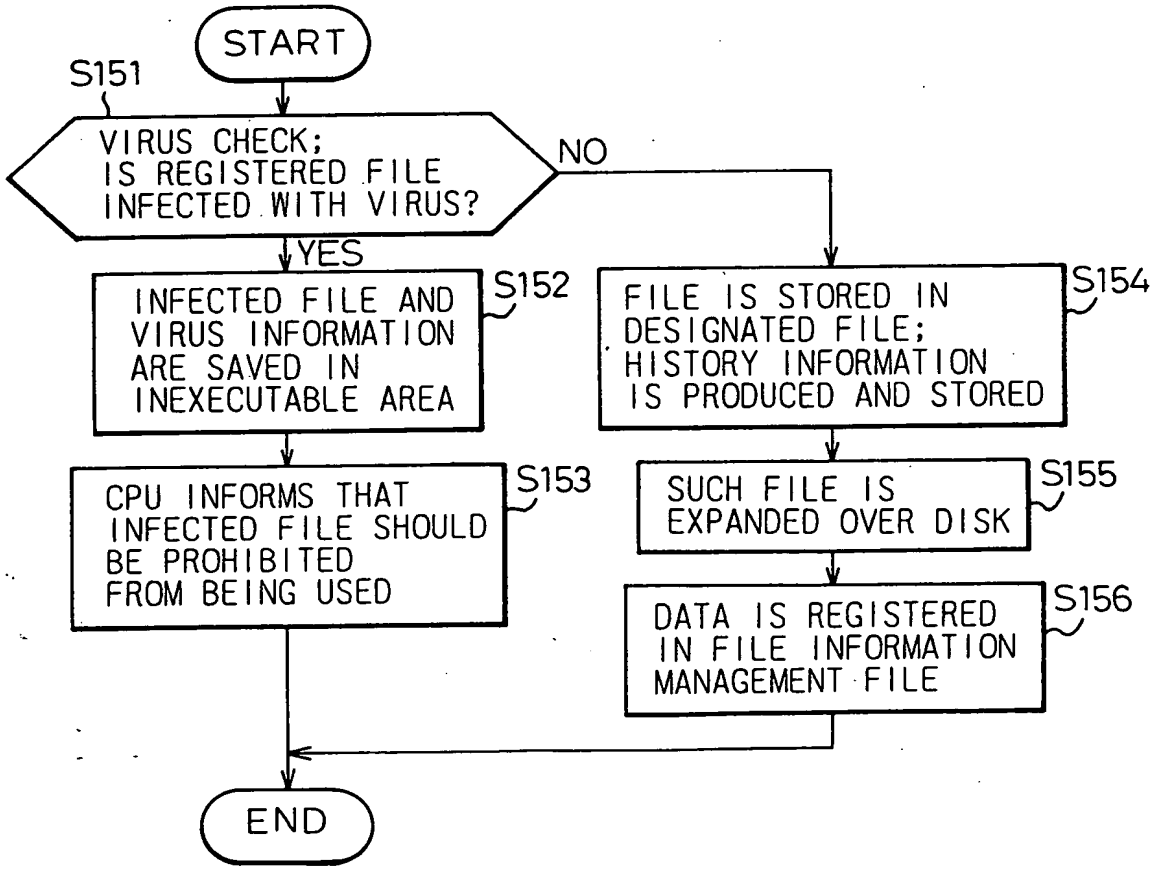

START
S151
VIRUS CHECK; IS REGISTERED FILE INFECTED WITH VIRUS?
NO
YES
INFECTED FILE AND VIRUS INFORMATION ARE SAVED IN INEXECUTABLE AREA
S152
CPU INFORMS THAT INFECTED FILE SHOULD BE PROHIBITED FROM BEING USED
S153
FILE IS STORED IN DESIGNATED FILE; HISTORY INFORMATION IS PRODUCED AND STORED
S154
SUCH FILE IS EXPANDED OVER DISK
S155
DATA IS REGISTERED IN FILE INFORMATION MANAGEMENT FILE
S156
END

Fig.16

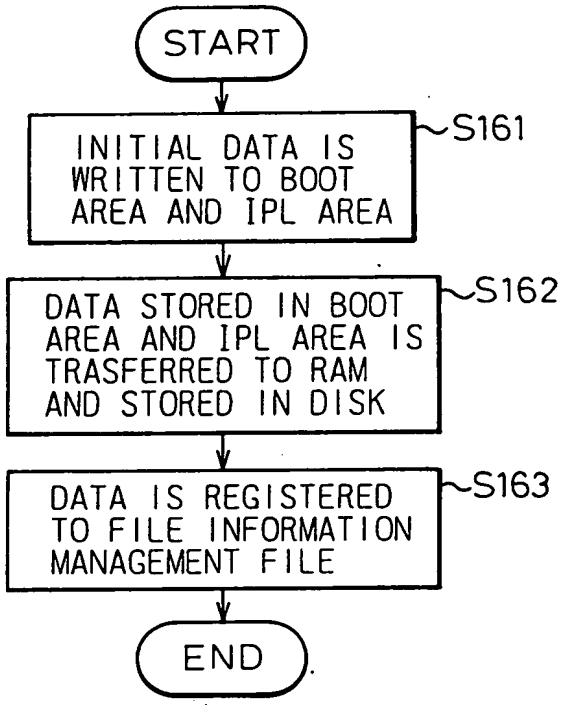

START
INITIAL DATA IS WRITTEN TO BOOT AREA AND IPL AREA
S161
DATA STORED IN BOOT AREA AND IPL AREA IS TRASFERRED TO RAM AND STORED IN DISK
S162
DATA IS REGISTERED TO FILE INFORMATION MANAGEMENT FILE
S163
END

Fig.17

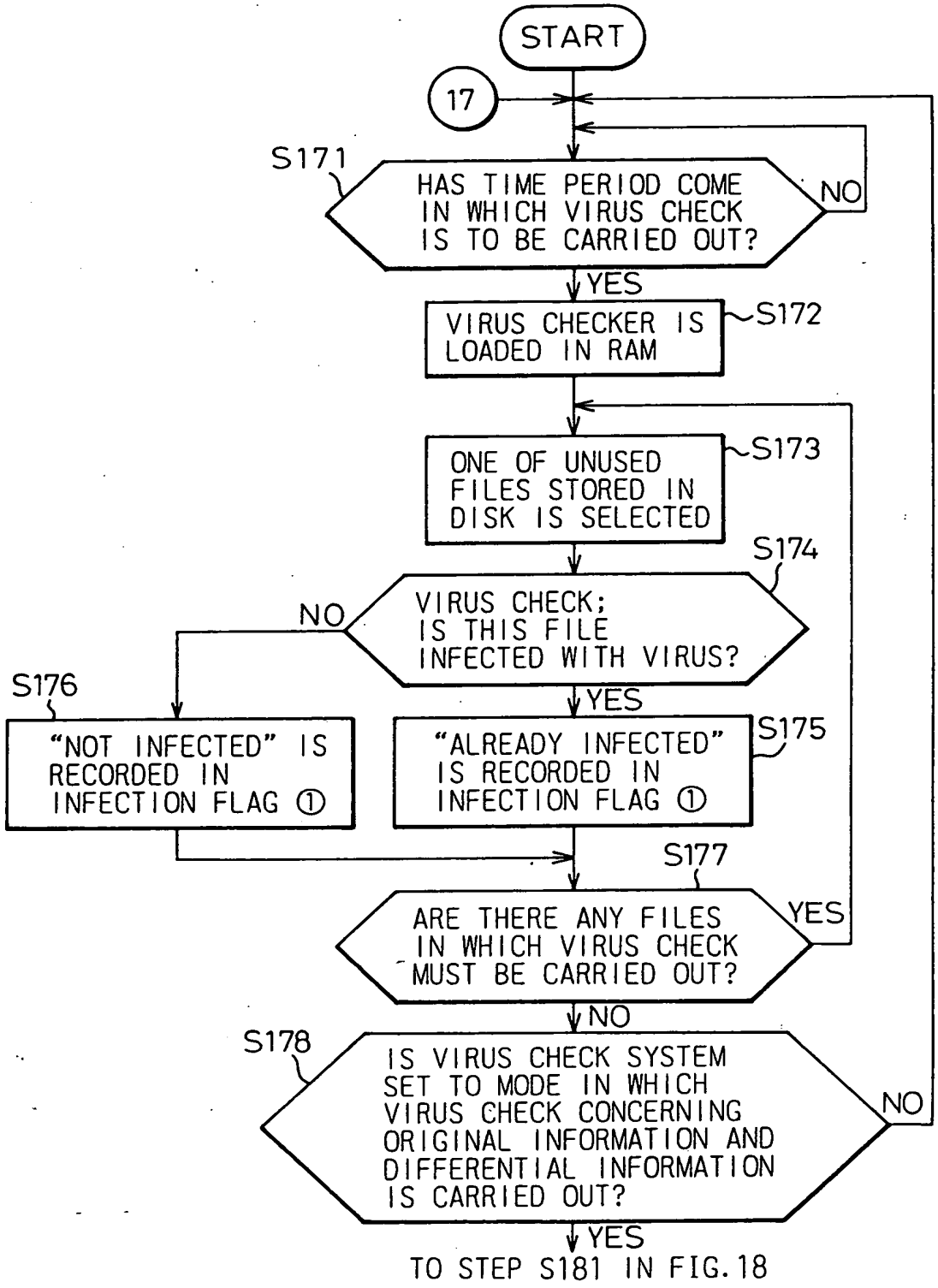

START
17
S171
HAS TIME PERIOD COME IN WHICH VIRUS CHECK IS TO BE CARRIED OUT?
NO
YES
VIRUS CHECKER IS LOADED IN RAM
S172
ONE OF UNUSED FILES STORED IN DISK IS SELECTED
S173
S174
VIRUS CHECK; IS THIS FILE INFECTED WITH VIRUS?
NO
YES
S176
"NOT INFECTED" IS RECORDED IN INFECTION FLAG ①
"ALREADY INFECTED" IS RECORDED IN INFECTION FLAG ①
S175
S177
ARE THERE ANY FILES IN WHICH VIRUS CHECK MUST BE CARRIED OUT?
YES
NO
S178
IS VIRUS CHECK SYSTEM SET TO MODE IN WHICH VIRUS CHECK CONCERNING ORIGINAL INFORMATION AND DIFFERENTIAL INFORMATION IS CARRIED OUT?
NO
YES
TO STEP S181 IN FIG. 18

Fig.18

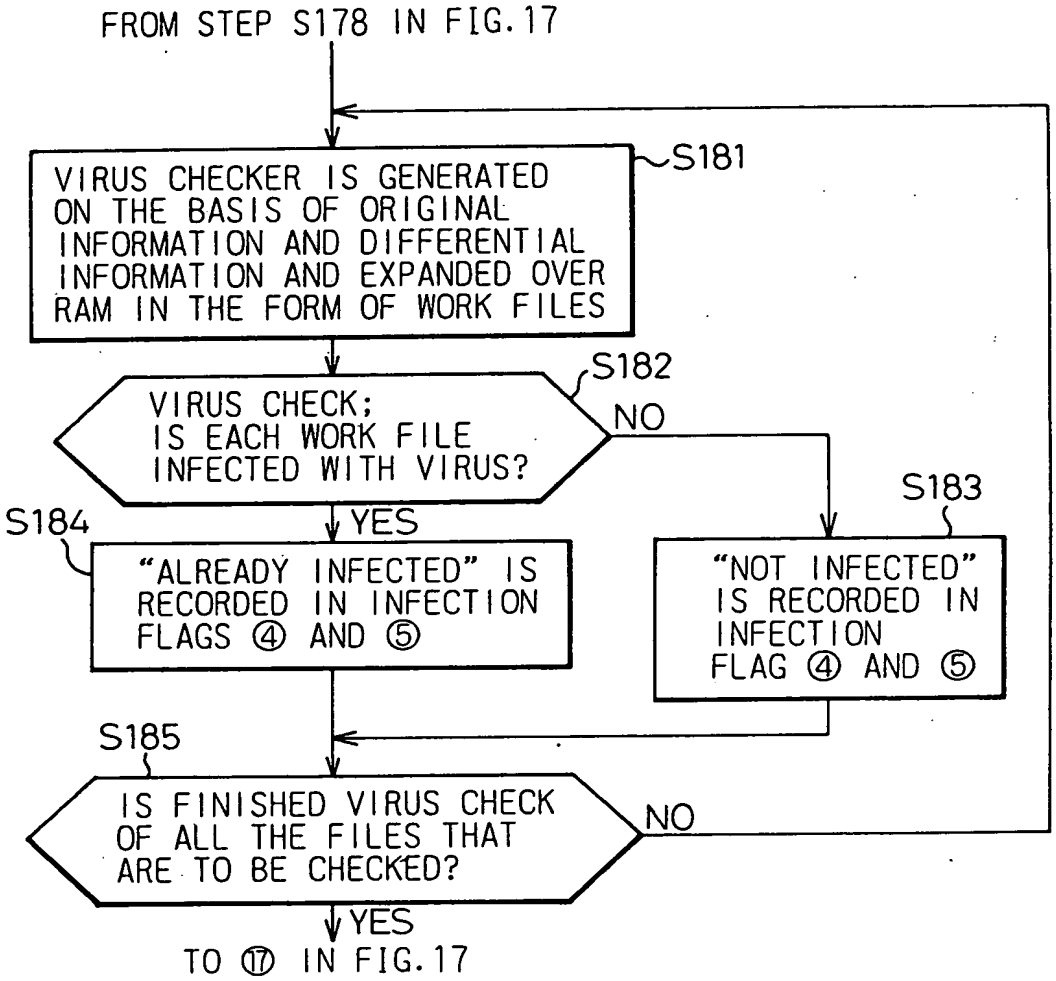

FROM STEP S178 IN FIG.17
VIRUS CHECKER IS GENERATED ON THE BASIS OF ORIGINAL INFORMATION AND DIFFERENTIAL INFORMATION AND EXPANDED OVER RAM IN THE FORM OF WORK FILES
S181
VIRUS CHECK; IS EACH WORK FILE INFECTED WITH VIRUS?
S182
NO
YES
S183
S184
"ALREADY INFECTED" IS RECORDED IN INFECTION FLAGS ④ AND ⑤
"NOT INFECTED" IS RECORDED IN INFECTION FLAG ④ AND ⑤
S185
IS FINISHED VIRUS CHECK OF ALL THE FILES THAT ARE TO BE CHECKED?
NO
YES
TO ⑰ IN FIG.17

Fig.19

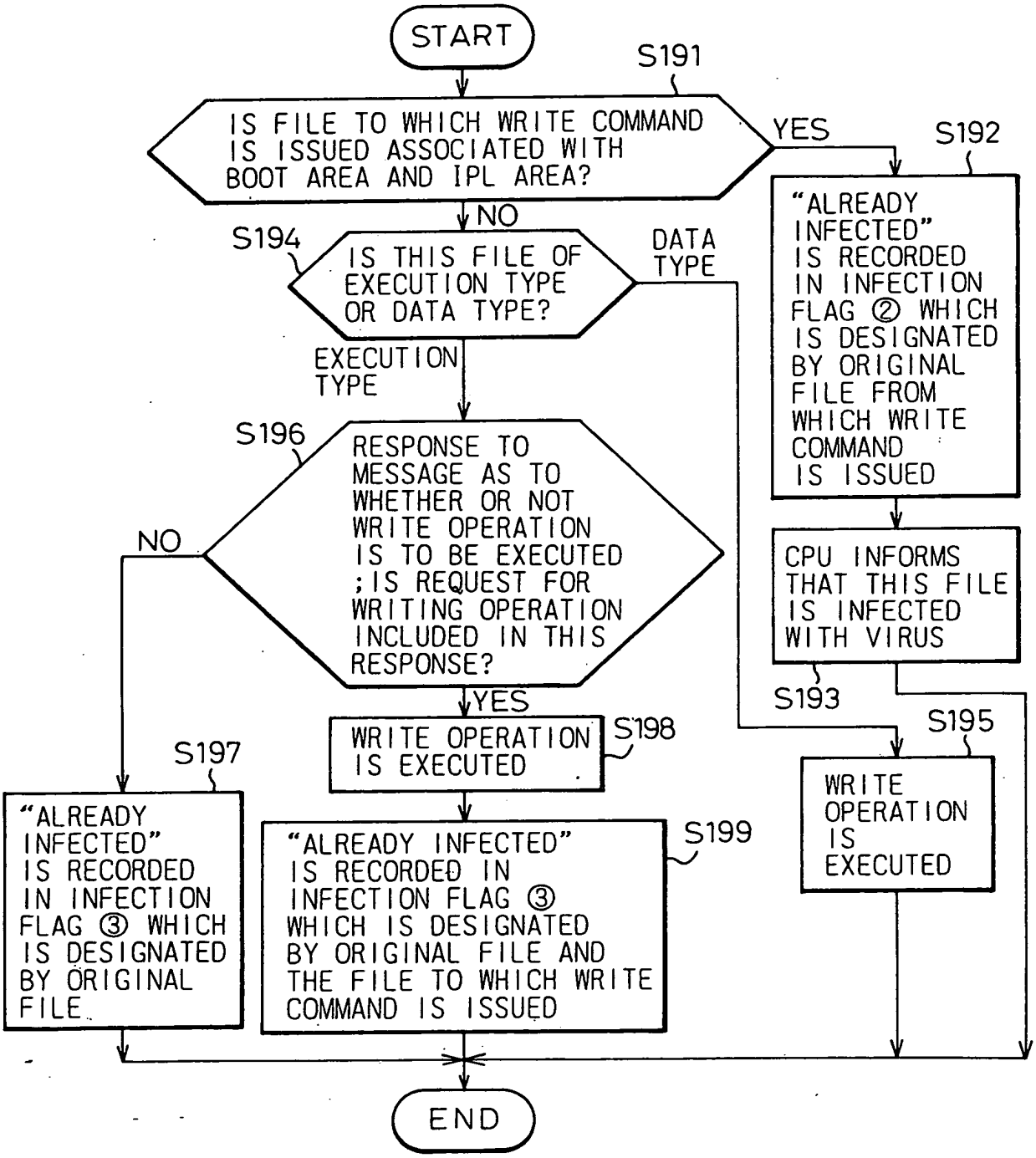

START
S191
IS FILE TO WHICH WRITE COMMAND IS ISSUED ASSOCIATED WITH BOOT AREA AND IPL AREA?
YES
S192
"ALREADY INFECTED" IS RECORDED IN INFECTION FLAG ② WHICH IS DESIGNATED BY ORIGINAL FILE FROM WHICH WRITE COMMAND IS ISSUED
NO
S194
IS THIS FILE OF EXECUTION TYPE OR DATA TYPE?
DATA TYPE
EXECUTION TYPE
S196
RESPONSE TO MESSAGE AS TO WHETHER OR NOT WRITE OPERATION IS TO BE EXECUTED ;IS REQUEST FOR WRITING OPERATION INCLUDED IN THIS RESPONSE?
NO
YES
CPU INFORMS THAT THIS FILE IS INFECTED WITH VIRUS
S193
S195
WRITE OPERATION IS EXECUTED
S198
WRITE OPERATION IS EXECUTED
S197
"ALREADY INFECTED" IS RECORDED IN INFECTION FLAG ③ WHICH IS DESIGNATED BY ORIGINAL FILE
S199
"ALREADY INFECTED" IS RECORDED IN INFECTION FLAG ③ WHICH IS DESIGNATED BY ORIGINAL FILE AND THE FILE TO WHICH WRITE COMMAND IS ISSUED
END

Fig.20

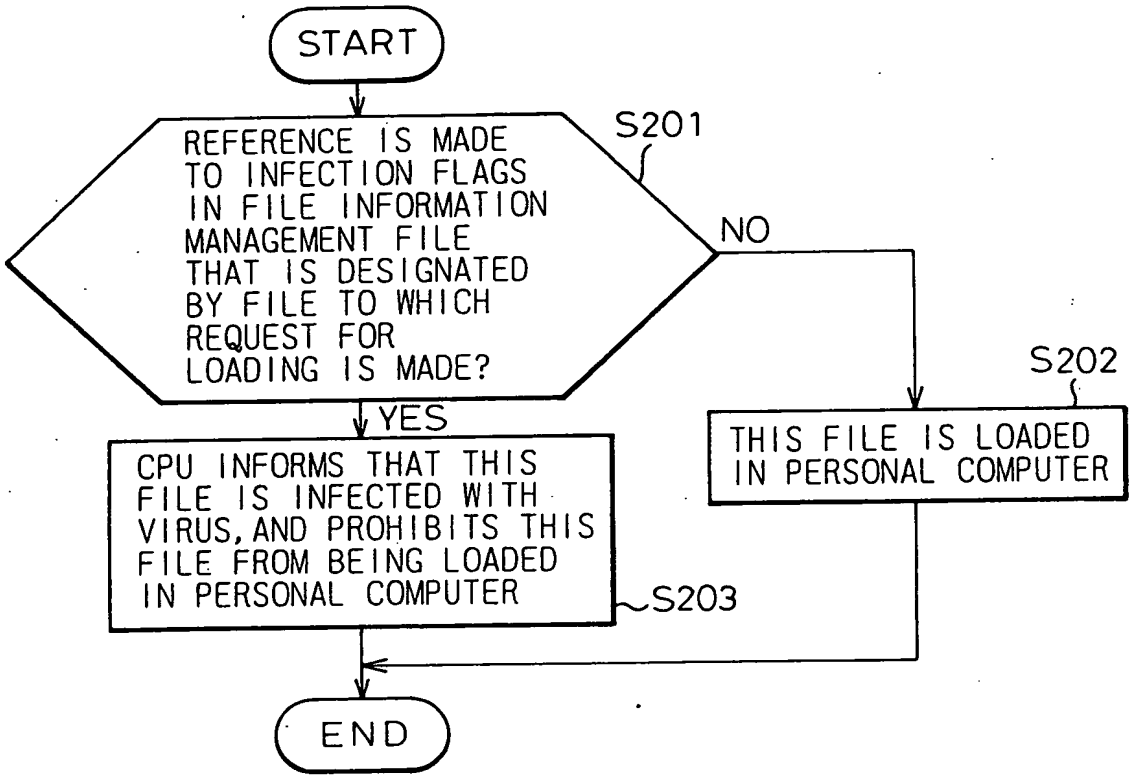

START
REFERENCE IS MADE TO INFECTION FLAGS IN FILE INFORMATION MANAGEMENT FILE THAT IS DESIGNATED BY FILE TO WHICH REQUEST FOR LOADING IS MADE?
S201
NO
YES
CPU INFORMS THAT THIS FILE IS INFECTED WITH VIRUS, AND PROHIBITS THIS FILE FROM BEING LOADED IN PERSONAL COMPUTER
S203
S202
THIS FILE IS LOADED IN PERSONAL COMPUTER
END

Fig.21

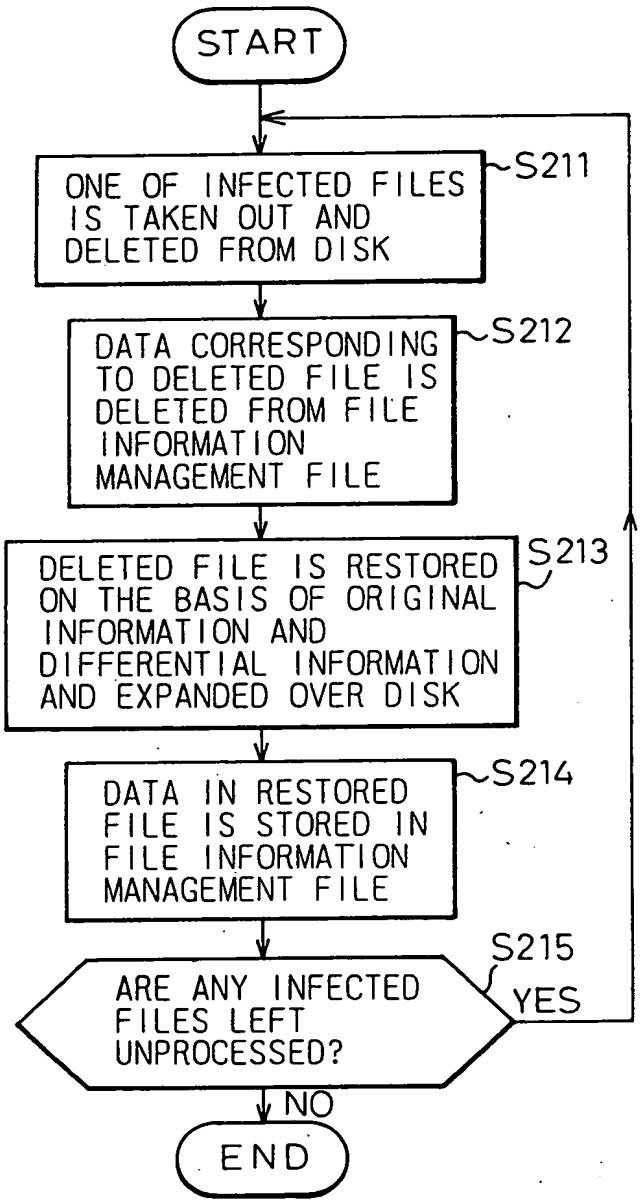

START
ONE OF INFECTED FILES IS TAKEN OUT AND DELETED FROM DISK
S211
DATA CORRESPONDING TO DELETED FILE IS DELETED FROM FILE INFORMATION MANAGEMENT FILE
S212
DELETED FILE IS RESTORED ON THE BASIS OF ORIGINAL INFORMATION AND DIFFERENTIAL INFORMATION AND EXPANDED OVER DISK
S213
DATA IN RESTORED FILE IS STORED IN FILE INFORMATION MANAGEMENT FILE
S214
ARE ANY INFECTED FILES LEFT UNPROCESSED?
S215
YES
NO
END

Fig.22

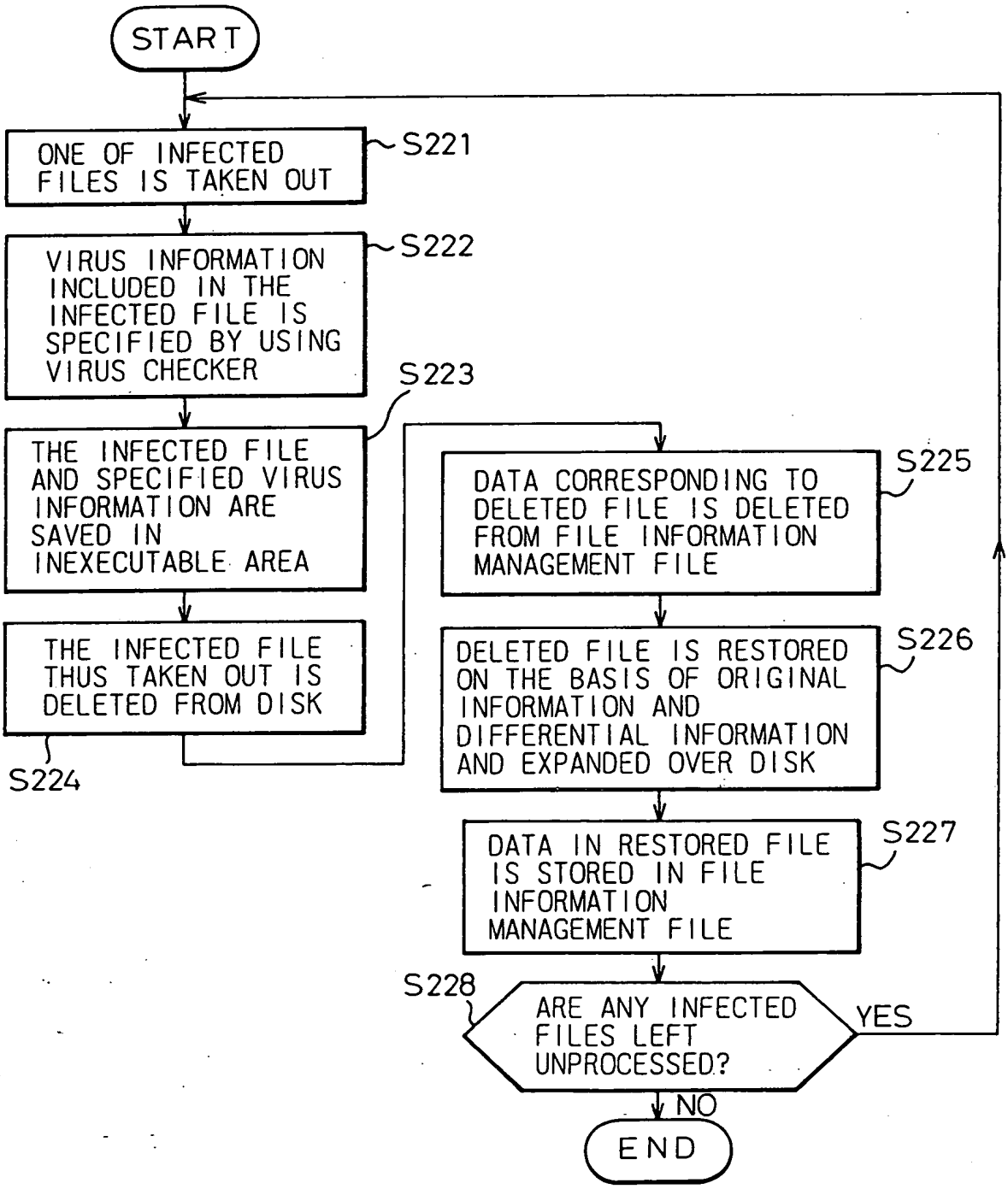

START
ONE OF INFECTED FILES IS TAKEN OUT
S221
VIRUS INFORMATION INCLUDED IN THE INFECTED FILE IS SPECIFIED BY USING VIRUS CHECKER
S222
THE INFECTED FILE AND SPECIFIED VIRUS INFORMATION ARE SAVED IN INEXECUTABLE AREA
S223
THE INFECTED FILE THUS TAKEN OUT IS DELETED FROM DISK
S224
DATA CORRESPONDING TO DELETED FILE IS DELETED FROM FILE INFORMATION MANAGEMENT FILE
S225
DELETED FILE IS RESTORED ON THE BASIS OF ORIGINAL INFORMATION AND DIFFERENTIAL INFORMATION AND EXPANDED OVER DISK
S226
DATA IN RESTORED FILE IS STORED IN FILE INFORMATION MANAGEMENT FILE
S227
S228
ARE ANY INFECTED FILES LEFT UNPROCESSED?
YES
NO
END

Fig.23

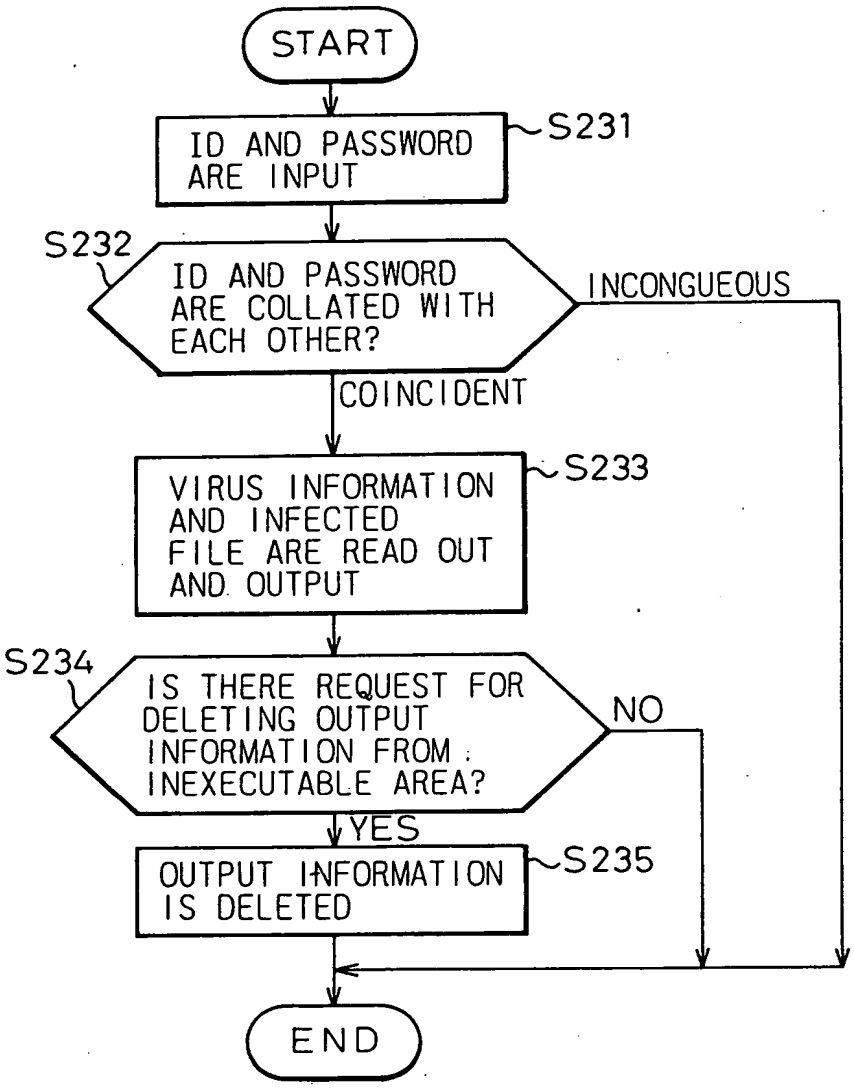

START
ID AND PASSWORD ARE INPUT
S231
S232
ID AND PASSWORD ARE COLLATED WITH EACH OTHER?
INCONGUEOUS
COINCIDENT
VIRUS INFORMATION AND INFECTED FILE ARE READ OUT AND OUTPUT
S233
S234
IS THERE REQUEST FOR DELETING OUTPUT INFORMATION FROM INEXECUTABLE AREA?
NO
YES
OUTPUT INFORMATION IS DELETED
S235
END

Fig.24

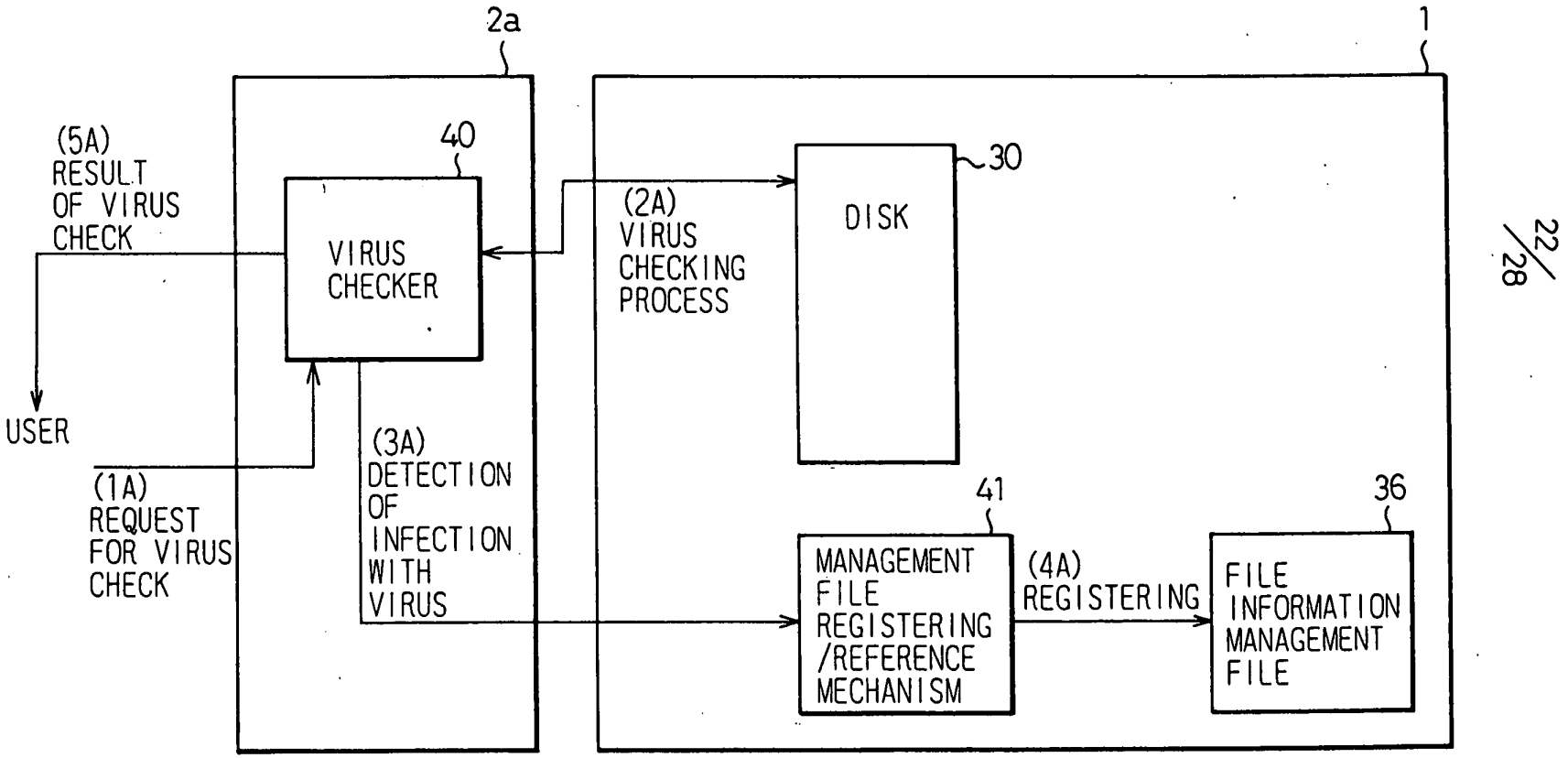

2a
1
40
30
(5A)
RESULT
OF VIRUS
CHECK
VIRUS
CHECKER
(2A)
VIRUS
CHECKING
PROCESS
DISK
USER
(1A)
REQUEST
FOR VIRUS
CHECK
(3A)
DETECTION
OF
INFECTION
WITH
VIRUS
41
36
MANAGEMENT
FILE
REGISTERING
/REFERENCE
MECHANISM
(4A)
REGISTERING
FILE
INFORMATION
MANAGEMENT
FILE

Fig.25

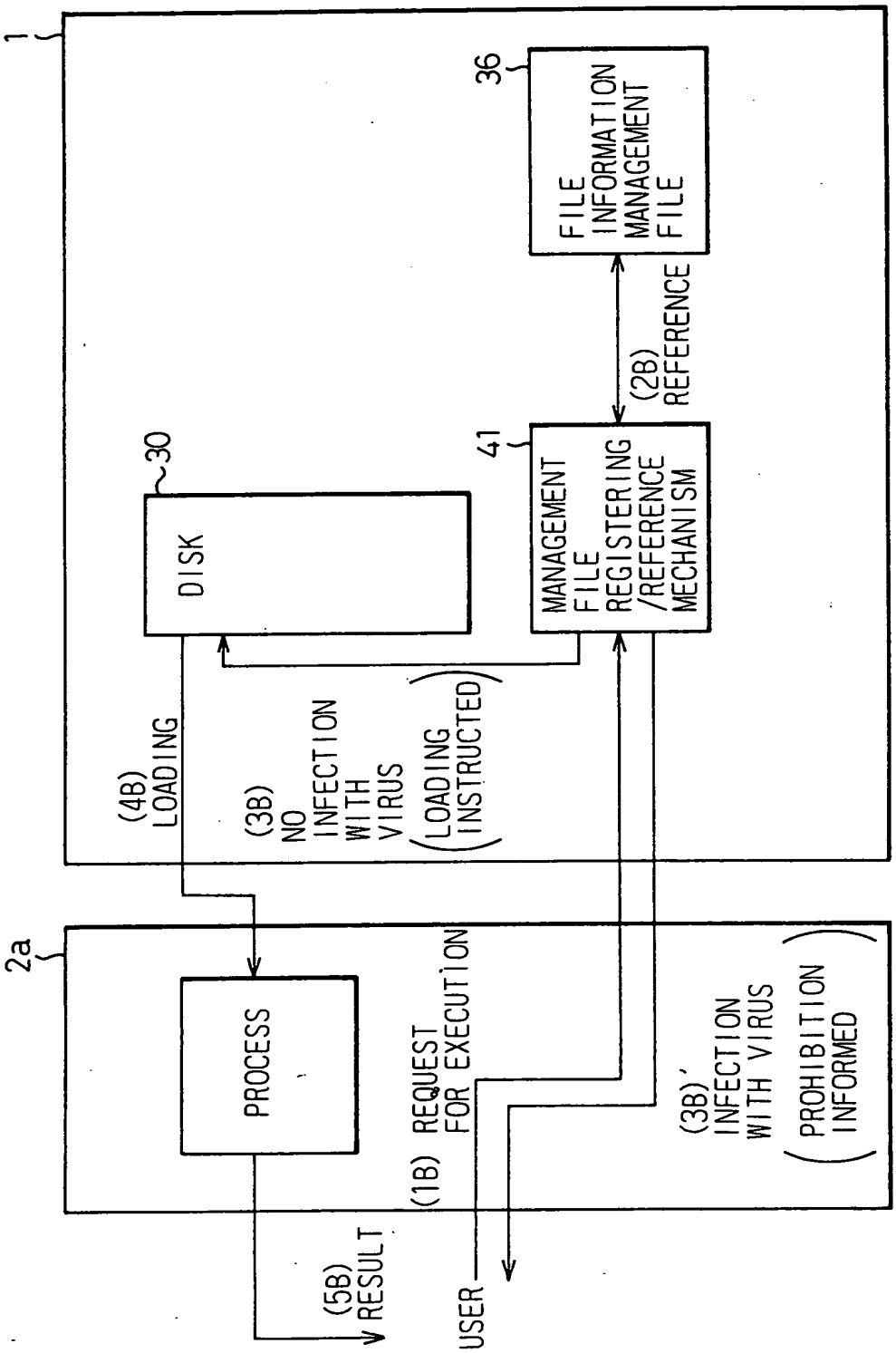

1
36
FILE INFORMATION MANAGEMENT FILE
(2B) REFERENCE
41
MANAGEMENT FILE REGISTERING /REFERENCE MECHANISM
30
DISK
(4B) LOADING
(3B) NO INFECTION WITH VIRUS
(LOADING INSTRUCTED)
2a
PROCESS
(1B) REQUEST FOR EXECUTION
(3B)' INFECTION WITH VIRUS
(PROHIBITION INFORMED)
(5B) RESULT
USER

Fig.26

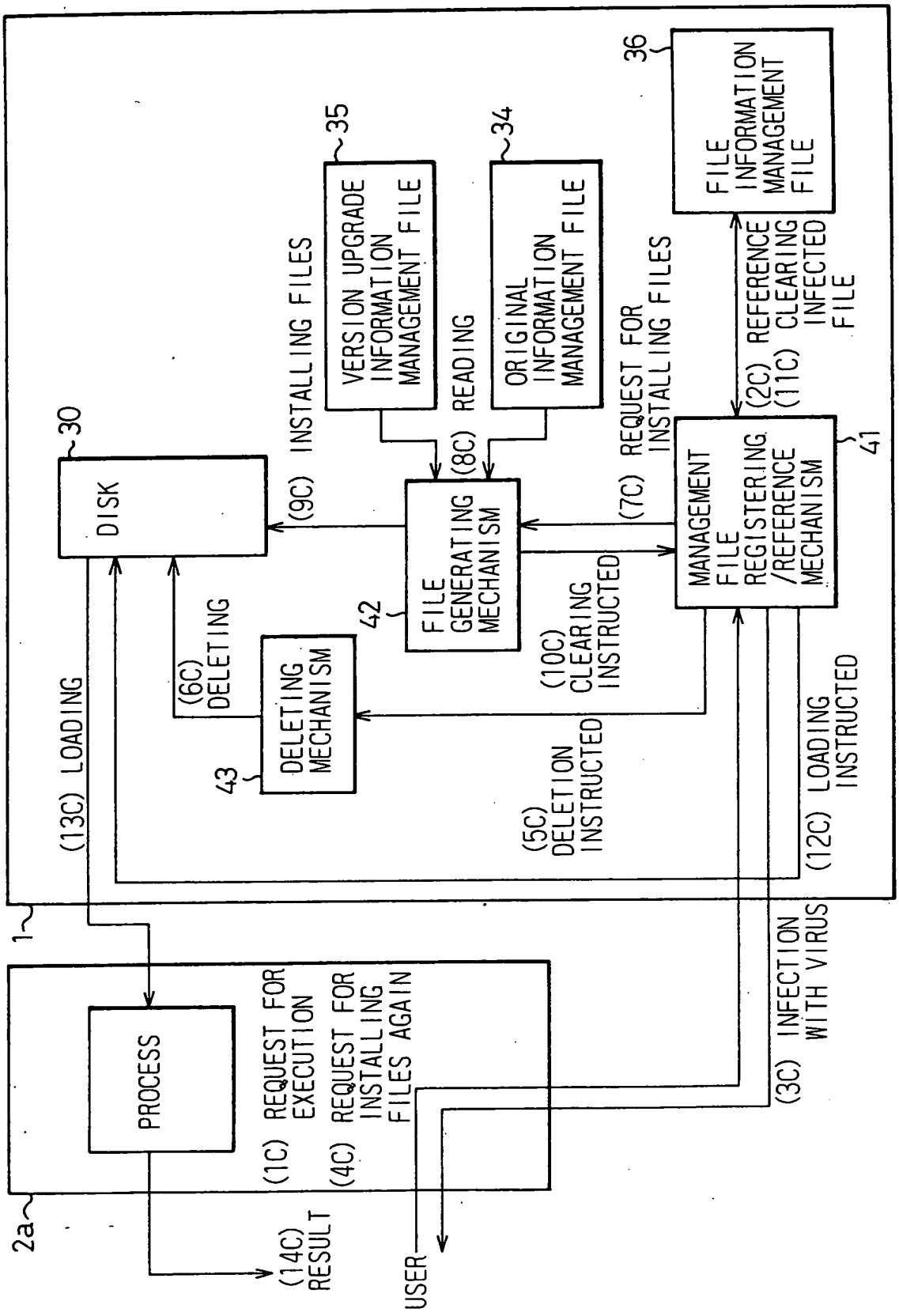

1
2a
PROCESS
(1C) REQUEST FOR EXECUTION
(4C) REQUEST FOR INSTALLING FILES AGAIN
(14C) RESULT
USER
(3C) INFECTION WITH VIRUS
(12C) LOADING INSTRUCTED
(5C) DELETION INSTRUCTED
(13C) LOADING
30
DISK
(6C) DELETING
43
DELETING MECHANISM
(9C) INSTALLING FILES
42
FILE GENERATING MECHANISM
(8C) READING
35
VERSION UPGRADE INFORMATION MANAGEMENT FILE
34
ORIGINAL INFORMATION MANAGEMENT FILE
(7C) REQUEST FOR INSTALLING FILES
(10C) CLEARING INSTRUCTED
MANAGEMENT FILE REGISTERING /REFERENCE MECHANISM
41
(2C) REFERENCE (11C) CLEARING INFECTED FILE
36
FILE INFORMATION MANAGEMENT FILE

Fig.27

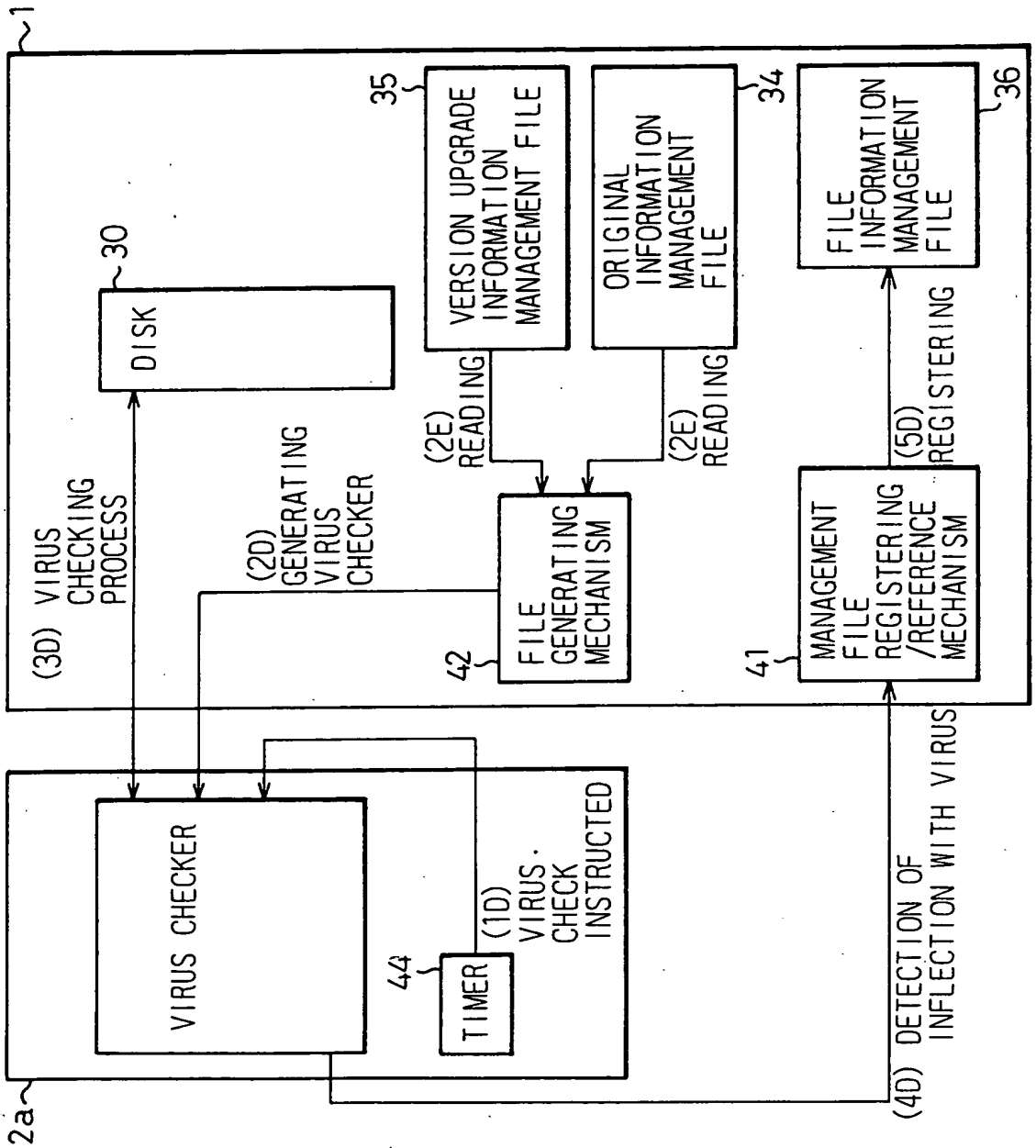

1
35
VERSION UPGRADE INFORMATION MANAGEMENT FILE
34
ORIGINAL INFORMATION MANAGEMENT FILE
36
FILE INFORMATION MANAGEMENT FILE
30
DISK
(3D) VIRUS CHECKING PROCESS
(2D) GENERATING VIRUS CHECKER
(2E) READING
(2E) READING
(5D) REGISTERING
42
FILE GENERATING MECHANISM
41
MANAGEMENT FILE REGISTERING /REFERENCE MECHANISM
VIRUS CHECKER
44
TIMER
(1D) VIRUS CHECK INSTRUCTED
(4D) DETECTION OF INFLECTION WITH VIRUS
2a

Fig.28

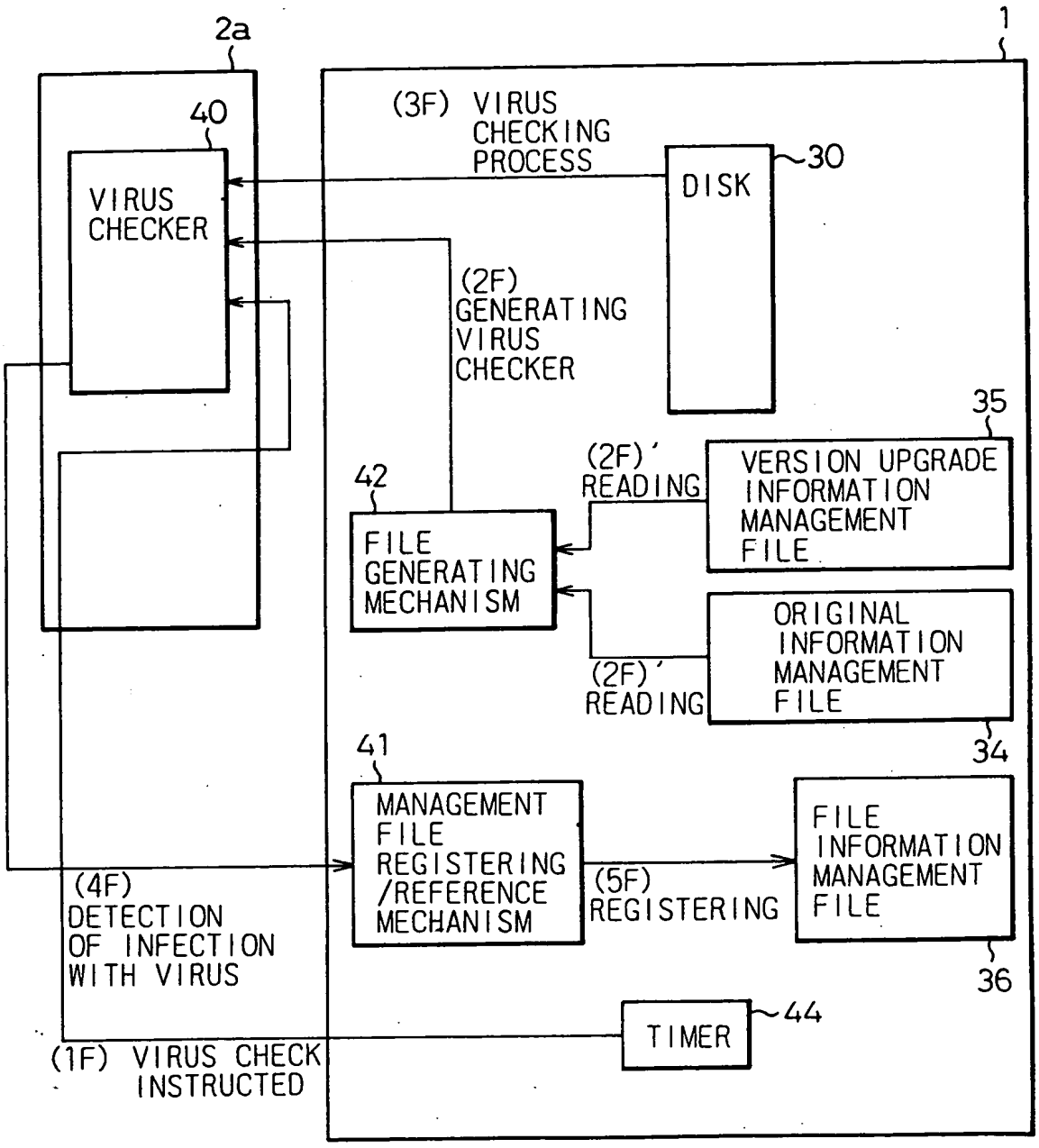

2a
1
40
VIRUS CHECKER
(3F) VIRUS CHECKING PROCESS
DISK
30
(2F) GENERATING VIRUS CHECKER
35
(2F)' READING
VERSION UPGRADE INFORMATION MANAGEMENT FILE
42
FILE GENERATING MECHANISM
ORIGINAL INFORMATION MANAGEMENT FILE
(2F)' READING
34
41
MANAGEMENT FILE REGISTERING /REFERENCE MECHANISM
(5F) REGISTERING
FILE INFORMATION MANAGEMENT FILE
36
(4F) DETECTION OF INFECTION WITH VIRUS
TIMER
44
(1F) VIRUS CHECK INSTRUCTED

Fig. 29

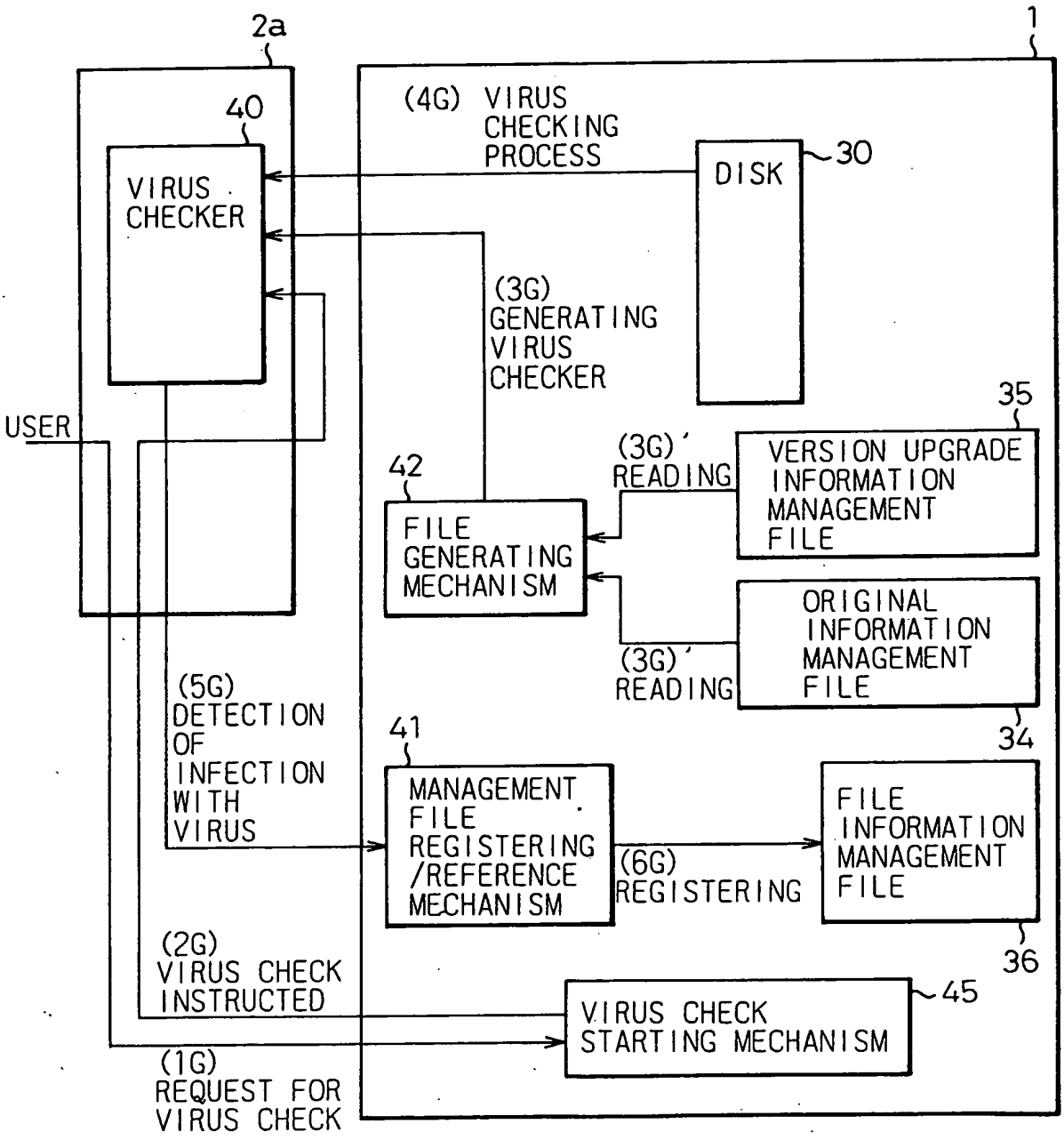
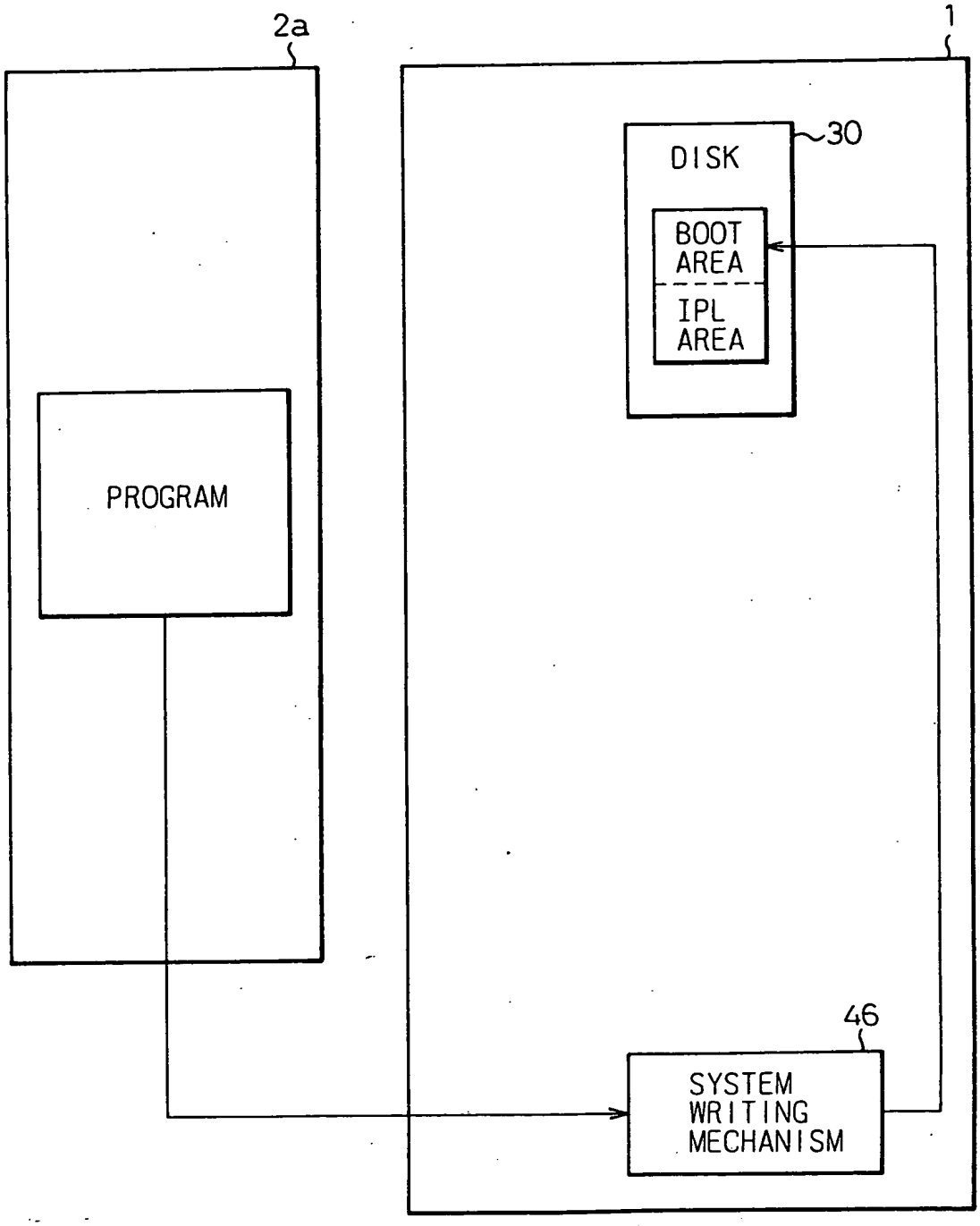

2a
1
40
VIRUS CHECKER
(4G) VIRUS CHECKING PROCESS
DISK
30
(3G) GENERATING VIRUS CHECKER
USER
35
(3G)' READING
VERSION UPGRADE INFORMATION MANAGEMENT FILE
42
FILE GENERATING MECHANISM
ORIGINAL INFORMATION MANAGEMENT FILE
(3G)' READING
34
(5G) DETECTION OF INFECTION WITH VIRUS
41
MANAGEMENT FILE REGISTERING /REFERENCE MECHANISM
(6G) REGISTERING
FILE INFORMATION MANAGEMENT FILE
36
(2G) VIRUS CHECK INSTRUCTED
45
VIRUS CHECK STARTING MECHANISM
(1G) REQUEST FOR VIRUS CHECK

Fig.30


2a
1
DISK
30
BOOT AREA
IPL AREA
PROGRAM
46
SYSTEM WRITING MECHANISM